



The Legal and Regulatory Framework for Payments in 14 SADC Member States Master Report

August 2014

Sarah Langan and Keith Smith
Prepared for FinMark Trust

PREFACE AND ACKNOWLEDGEMENTS

This report was commissioned by FinMark Trust with the support of the SADC Payment System Subcommittee and Committee of Central Bank Governors (CCBG) Legal Subcommittee as the first step in a long journey towards a harmonised legal and regulatory framework for payments in the SADC. This report consists of a Master Report and two volumes of country reports.¹

The authors are grateful for the level of cooperation and assistance provided by every person with whom we consulted during the research phase of this project. We especially acknowledge the willingness of those who made themselves available, often at very short notice in all fourteen SADC countries, to answer multitudinous questions, search for and provide numerous documents and generally provide the information that was requested. In this regard, we acknowledge and thank all those with whom we met. (See the [full list of individuals interviewed](#) during the first half of 2013.)

We would also like to thank the following individuals and organisations for providing commentary on the first draft of the following sections of the report:

VOLUME I: SADC COUNTRY REPORTS (ANNEXURES A – G)

- Annexure A:** Mr. Victor Rodrigues, Head of Projects Banco Nacional de Angola
- Annexure B:** Mrs. Ewetse Rakhudu, Director of the Payments and Settlement Department of the Bank of Botswana
- Annexure C:** Mr. Kapinga Tshimanga and Mr. Mukengeshay Katalay (Banque Centrale du Congo)
- Annexure D:** Mr. S Ntelo, Director of Operations Central Bank of Lesotho; Mr. Grey Nkungula, Payment Systems Advisor Central Bank of Lesotho; Mr. Motheo Lechesa, Head NPS Central Bank of Lesotho and Ms. Limpho Linake, Legal Officer Central Bank of Lesotho
- Annexure E:** Mr. Fraser Mdwazika, Director National Payments System Reserve Bank of Malawi; Mr. Osky Sichinga, Manager Policy and Settlements Reserve Bank of Malawi; Mr. George Chioza, Manager Legal Services Reserve Bank of Malawi and Ms. Agnes Sentala, Legal Counsel Reserve Bank of Malawi
- Annexure G:** Ms. Aurora Billa and her team from the Banco de Moçambique

VOLUME II: SADC COUNTRY REPORTS (ANNEXURES H – N)

- Annexure H:** Ms. Barbara Gowaseb, Director: Payment and Settlement Systems Bank of Namibia; Mr. Tulonga Nakamelah, Head: Legal Services and Contract Management Bank of Namibia; Mr. Sergio de Sousa, Deputy Director: Oversight, Policy and Research Bank of Namibia

¹ This document has been prepared in good faith on the basis of information available at the date of publication. Readers are responsible for assessing the relevance and accuracy of the content. FinMark Trust and the authors will not be liable for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on information in this publication.

- Annexure I:** The team from the National Payment Systems Unit Central Bank of Seychelles
- Annexure J:** The team from the South African Reserve Bank Legal Services Department and National Payment Systems Department
- Annexure L:** Mrs. Lucy Kinunda and Mr. George Sije (Bank of Tanzania)
- Annexure M:** The team from the Bank of Zambia

SECTIONS OF THE MASTER REPORT

- AML sections 3.1.3 and 9** Professor Louis De Koker (Deakin University), Mr. Tom Maliku (ESAAMLG) and Mr. Benjamin Musuku (World Bank)

TABLE OF CONTENTS

PREFACE AND ACKNOWLEDGEMENTS	ii
TABLE OF CONTENTS	iv
TABLES IN THE MASTER REPORT	xi
DIAGRAMS IN THE MASTER REPORT	xiv
EXECUTIVE SUMMARY	xv
SECTION 1: INTRODUCTION	1
SECTION 2: HARMONISATION OF PAYMENT SYSTEM LAWS IN SADC	5
2.1 The SADC Institutions and Structures	6
2.1.1 The Summit	6
2.1.2 The Council of Ministers.....	7
2.1.3 The Integrated Committee of Ministers.....	8
2.1.4 The Standing Committee of Officials (SCO)	8
2.1.5 The Secretariat.....	8
2.1.6 The Summit Troika	8
2.1.7 The Committee of Central Bank Governors.....	8
2.1.8 The Tribunal.....	9
2.1.9 The SADC Parliamentary Forum.....	9
2.2 Legal Status of SADC Instruments.....	10
2.2.1 The SADC Treaty and Protocols	10
2.2.2 SADC Model Laws	11
2.2.3 The Legal Status of MOU's and TA's	11
2.3 The Basis for Harmonisation of Payment System Law in SADC	12
2.3.1 Annex 6 of the Protocol on Financial and Investment (FIP)	12
2.3.2 Annex 12 of the Protocol on Financial and Investment (FIP)	13
2.3.3 The Cooperation Framework Annex 6 of the FIP.....	14
2.3.4 Institutional Challenges – Annex 12 of the FIP	15
2.4 Prior Considerations Before Embarking Upon Harmonisation of Payment System Law.....	15
2.4.1 Differing Legal Traditions	15

2.4.2	Different Regulatory Models Applied by SADC Member States	17
2.4.3	Different Levels of Infrastructural Development	21
SECTION 3: INTERNATIONAL BEST PRACTICE: CHOICE OF BENCHMARKS		24
3.1	International Standards (Soft Laws)	24
3.1.1	The CPSIPS and PFMI's	25
3.1.1.1	<i>Core Principles for Systemically Important Payment Systems (CPSIPS)</i>	25
3.1.1.2	<i>Recommendations for Securities Settlement Systems (RSSS)</i>	26
3.1.1.3	<i>Recommendations for Central Counterparties (RCCP)</i>	26
3.1.1.4	<i>Principles for Financial Market Infrastructures (PFMI)</i>	26
3.1.2	UNCITRAL Model Law on Electronic Commerce (1996)	29
3.1.3	The FATF Recommendations (2012)	34
3.1.3.1	FATF Recommendation 1: Assessing Risks and Applying the Risk Based Approach	35
3.1.3.1.1	<i>The Proven Low Risk Exemption</i>	36
3.1.3.1.2	<i>The De Minimus Exemption</i>	38
3.1.3.1.3	<i>The Lower Risk Scenarios</i>	40
3.1.3.1.4	<i>Higher Risk</i>	40
3.1.3.2	FATF Recommendation 10: Customer Due Diligence	41
3.1.3.3	FATF Recommendation 11: Record Keeping	43
3.1.3.4	FATF Recommendation 13: Correspondent Banking	44
3.1.3.5	FATF Recommendation 14: Money or Value Transfer Services	44
3.1.3.6	FATF Recommendation 15: New Technologies	45
3.1.3.7	FATF Recommendation 16: Wire Transfers	45
3.1.3.8	FATF Recommendation 17: Reliance on Third Parties	46
3.1.3.9	FATF Recommendation 20: Suspicious Transaction Reporting	47
3.1.3.10	FATF Recommendation 34: Guidance and Feedback	48
3.1.4	The BIS/World Bank General Principles for International Remittance Services	48
3.2	European Union Regulations and Directives (Hard Law)	49
3.2.1	The EC Regulations	52
3.2.1.1	Regulation (EC) No 924/2009 Cross-border Payments in the Community	53
3.2.1.2	Regulation EC No 178/2006 Information on the Payer Accompanying Transfers of Funds	55
3.2.1.3	Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and	

Direct Debits in Euro	57
3.2.2 The Directives	61
3.2.2.1 Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC)	63
3.2.2.2 Electronic Signatures Directive 1999/93/EC	67
3.2.2.3 Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions	71
3.2.2.4 Directive 2004/39/EC Markets in Financial Instruments (MiFID).....	76
3.2.2.5 Directive 2007/64/EC Payment Services in the Internal Market (PSD)	77
3.2.2.5.1 <i>Subject Matter of the Directive</i>	77
3.2.2.5.2 <i>Application for Authorisation as a Payment Institution</i>	80
3.2.2.5.3 <i>Initial Capital</i>	80
3.2.2.5.4 <i>Own Funds</i>	81
3.2.2.5.5 <i>Safeguarding Requirements</i>	81
3.2.2.5.6 <i>Granting of Authorisation</i>	82
3.2.2.5.7 <i>Withdrawal of Authorisation</i>	82
3.2.2.5.8 <i>Public Register of Authorised Payment Institutions, their Agents and Branches</i>	82
3.2.2.5.9 <i>Accounting and Statutory Audit</i>	82
3.2.2.5.10 <i>Use of Agents, Branches or Entities to which Activities are Outsourced</i>	82
3.2.2.5.11 <i>Liability</i>	83
3.2.2.5.12 <i>Record Keeping</i>	83
3.2.2.5.13 <i>Designation of Competent Authorities</i>	83
3.2.2.5.14 <i>Supervision</i>	84
3.2.2.5.15 <i>Professional Secrecy</i>	84
3.2.2.5.16 <i>Right to Apply to the Courts</i>	85
3.2.2.5.17 <i>Exchange of information</i>	85
3.2.2.5.18 <i>Exercise of the Right of Establishment and Freedom to Provide Services</i>	85
3.2.2.5.19 <i>Waiver</i>	85
3.2.2.5.20 <i>Notification and Information (Waiver)</i>	86
3.2.2.5.21 <i>Access to Payment Systems</i>	86
3.2.2.5.22 <i>Prohibition for Persons other than Payment Service Providers to Provide Payment Services</i>	87
3.2.2.5.23 <i>Charges for Information</i>	88
3.2.2.5.24 <i>Burden of Proof on Information Requirements</i>	88

3.2.2.5.25	<i>Derogation from Information Requirements for Low-value Payment Instruments and Electronic Money</i>	88
3.2.2.5.26	<i>Single Payment Transaction – Prior General Information</i>	89
3.2.2.5.27	<i>Single Payment Transaction - Information and Conditions</i>	89
3.2.2.5.28	<i>Single Payment Transaction - Information for the Payer after Receipt of the Payment Order</i>	90
3.2.2.5.29	<i>Single Payment Transaction - Information for the Payee After Execution</i>	90
3.2.2.5.30	<i>Framework Contracts - Prior General Information</i>	90
3.2.2.5.31	<i>Framework Contracts - Information and Conditions</i>	91
3.2.2.5.32	<i>Framework Contracts - Accessibility of Information and Conditions of the Framework Contract</i>	93
3.2.2.5.33	<i>Framework Contracts - Changes in Conditions of the Framework Contract</i>	93
3.2.2.5.34	<i>Framework Contracts – Termination</i>	93
3.2.2.5.35	<i>Framework Contracts - Information Before Execution of Individual Payment Transactions</i>	93
3.2.2.5.36	<i>Framework Contracts - Information for the Payer on Individual Payment Transactions</i>	94
3.2.2.5.37	<i>Framework Contracts - Information for the Payee on Individual Payment Transactions</i>	94
3.2.2.5.38	<i>Common Provisions - Currency and Currency Conversion</i>	94
3.2.2.5.39	<i>Common Provisions - Information on Additional Charges or Reductions</i>	95
3.2.2.5.40	<i>Charges Applicable</i>	96
3.2.2.5.41	<i>Derogation for Low Value Payment Instruments and Electronic Money</i>	96
3.2.2.5.42	<i>Authorisation of Payment Transactions – Consent and Withdrawal of Consent</i>	97
3.2.2.5.43	<i>Authorisation of Payment Transactions – Limits of the Use of the Payment Instrument</i>	98
3.2.2.5.44	<i>Obligations of the Payment Service User in Relation to Payment Instruments</i>	98
3.2.2.5.45	<i>Obligations of the Payment Service Provider in Relation to Payment Instruments</i>	98
3.2.2.5.46	<i>Notification of Unauthorised or Incorrectly Executed Payment Transactions</i>	99
3.2.2.5.47	<i>Evidence on Authentication and Execution of Payment Transactions</i>	99
3.2.2.5.48	<i>Payment Service Provider's Liability for Unauthorised Payment Transactions</i>	99
3.2.2.5.49	<i>Payer's Liability for Unauthorised Payment Transactions</i>	100
3.2.2.5.50	<i>Refunds for Payment Transactions Initiated by or Through a Payee</i>	100
3.2.2.5.51	<i>Requests for Refunds for Payment Transactions Initiated by or Through a Payee</i>	101
3.2.2.5.52	<i>Payment Orders and Amounts Transferred – Receipt of Payment Orders</i>	101
3.2.2.5.53	<i>Refusal of Payment Orders</i>	101
3.2.2.5.54	<i>Irrevocability of a Payment Order By a Payment Service User</i>	101

3.2.2.5.55	<i>Amounts Transferred and Amounts Received</i>	102
3.2.2.5.56	<i>Execution Time and Value Date</i>	102
3.2.2.5.57	<i>Payment Transactions to a Payment Account</i>	102
3.2.2.5.58	<i>Absence of Payee's Payment Account with the Payment Service Provider</i>	103
3.2.2.5.59	<i>Cash Placed on a Payment Account</i>	103
3.2.2.5.60	<i>National Payment Transactions</i>	103
3.2.2.5.61	<i>Value Date and Availability of Funds</i>	103
3.2.2.5.62	<i>Liability - Incorrect Unique Identifiers</i>	103
3.2.2.5.63	<i>Liability - Non-execution or Defective Execution</i>	104
3.2.2.5.64	<i>Right of Recourse</i>	104
3.2.2.5.65	<i>Data Protection</i>	104
3.2.2.5.66	<i>Complaint Procedures</i>	105
3.2.2.5.67	<i>Penalties</i>	105
3.2.2.5.68	<i>Complaints Procedure to be Administered by Competent Authorities</i>	105
3.2.2.5.69	<i>Out-of-Court-Redress</i>	105
SECTION 4: DOMESTIC LEGAL AND REGULATORY FRAMEWORKS IN SADC		110
4.1	A Sound Legal Basis	110
4.2	Legislation and Regulation (Overarching Gap Analysis)	113
4.3	Strong Legal Influence (National Payment System Acts)	119
4.3.1	Similar Acts: South Africa, Namibia and Lesotho	120
4.3.2	Almost Identical Acts: Botswana, Seychelles and Swaziland	123
4.3.3	Similar Acts: Mozambique and Angola	125
4.3.4	Unique Acts: Zambia's National Payment Systems Act, 2007	128
4.3.5	Unique Bill: Malawi's National Payment Systems Bill	130
4.3.6	Unique Draft Act: The DRC's Draft Law on the Provisions Applicable to the NPS	132
SECTION 5: REVIEW OF EACH MEMBER STATE'S PRIMARY PAYMENT STATUTE		136
5.1	Definitions	137
5.1.1	Comparative Review (Definitions in Domestic Law)	138
5.1.2	Measurement of Terms in Domestic Legislation against International Best Practice (EU Directives)	143
5.1.3	Measurement against International Best Practice (The EU Regulations)	146
5.2	The Role of the Central Bank in the National Payment System	148

5.2.1	Powers, Functions, Regulation and Oversight by the Central Bank	148
5.2.1.1	<i>Powers and Functions of the Central Bank with respect to the National Payment System as set out in the Central Bank Law</i>	148
5.2.1.2	<i>Powers and Functions of the Central Bank with respect to the National Payment System as set out in the National Payment System Act</i>	152
5.3	Confidentiality, Disclosure of Information and Indemnity	163
5.4	The Public Interest Objective	164
5.5	Access to Clearing and Settlement Systems	166
5.6	Settlement Finality and Irrevocability	177
5.7	Transfer Orders and Netting	178
5.7.1	Transfer Orders and Netting Are Legally Enforceable and Binding on Third Parties	179
5.7.2	No Law, Regulation or Rule Will Result in the Unwinding of Netting	188
5.7.3	Interoperable Systems	190
5.8	Provisions Concerning Insolvency	190
5.8.1	The Moment of Opening of Insolvency Proceedings	190
5.8.2	Notification of the Decision to the Central Bank	192
5.8.3	Notification of the Decision to Other Member States	195
5.8.4	No Retroactive Effects	196
5.9	Collateral Security	198
5.10	Prohibition against Payment Intermediation	202
5.11	Conflict of Laws	203
5.12	Dispute Resolution	204
5.12.1	<i>Domestic Arbitration</i>	204
5.12.2	<i>International Arbitration</i>	206
SECTION 6: ELECTRONIC DOCUMENTS, TRANSACTIONS AND SIGNATURES		208
6.1	Scope and Content of Relevant Provisions found in the South African Electronic Communications and Transactions Act, 2002	209
6.2	Level of Compliance SADC Member States Act with International Best Practice	217
SECTION 7: ELECTRONIC MONEY		220
7.1	The Current State of Play in SADC	220
7.2	The Scope and Content of Namibia’s Payment System Determination (PSD-3)	223

7.3 Level of Compliance with International and Regional Best Practice	230
SECTION 8: PAYMENT SERVICES	233
SECTION 9: ANTI-MONEY LAUNDERING	248
9.1 Level of Compliance with Recommendation 10: CDD	248
9.1.1 Component A: When is CDD Required?	248
9.1.2 Component B: Identification Measures and Verification Sources	262
9.1.3 Component C: The Timing and Verification of Identity	276
9.1.4 The Risk-Based Approach to CDD: The Proven Low Risk Exemption and Simplified Measures	279
9.2 Level of Compliance with Recommendation 11: Record Keeping	295
9.3 Level of Compliance with Recommendation 13: Correspondent Banking	302
9.7 Level of Compliance with Recommendation 20: STRs	326
9.8 Level of Compliance with Recommendation 34: Guidance and Feedback	336
SECTION 10: RECOMMENDATIONS	340
10.1 SADC Wide Findings and Recommendations	340
Recommendation 1: Glossary of Key Terms	341
Recommendation 2: Model Laws (National Payment System and Payment Services)	342
Recommendation 3: Model Law (AML/CFT)	342
Recommendation 4: Scoping Study and Preparation of an Electronic Money Guideline for SADC	343
10.2 Country Specific Recommendations	343
ANNEXURE O: TRANSPOSITION OF THE SETTLEMENT FINALITY DIRECTIVE	345
ANNEXURE P: TRANSPOSITION OF THE ELECTRONIC SIGNATURES DIRECTIVE	348
ANNEXURE Q: TRANSPOSITION OF THE E-MONEY DIRECTIVE	353
ANNEXURE R: TRANSPOSITION OF THE PSD	368
INDIVIDUALS INTERVIEWED	403
ACRONYMNS	410
REFERENCES	414

TABLES

Table 1: Legal Traditions in SADC Countries.....	17
Table 2: Regulatory Models.....	18
Table 3: Regulatory Models Applied in SADC.....	19
Table 4: Functions Delegated to the PSMB in South Africa.....	20
Table 5: FMI Infrastructure in SADC (RTGS).....	22
Table 6: FMI Infrastructure in SADC (Other).....	23
Table 7: Other Relevant Infrastructure Related Data.....	23
Table 8: Ten Core Principle for Systemically Important Payment Systems and Four Responsibilities of Central Banks in Applying Them.....	25
Table 9: General Applicability of Principles to Specific Types of FMIs.....	27
Table 10: Responsibilities of Central Banks, Market Regulators and Other Relevant Authorities.....	29
Table 11: UNCITRAL Model Law on Electronic Commerce (1996).....	30
Table 12: Five Principles for International Remittance Services.....	48
Table 13: Examples of the National Application of Settlement Finality Directive.....	66
Table 14: Examples of the National Application of Electronic Signatures Directive.....	69
Table 15: Activities that Electronic Money Issuers May Engage In.....	73
Table 16: Examples of the National Application of the E-Money Directive.....	75
Table 17: Payment Services to which the PSD applies (“The Annex”).....	78
Table 18: Negative Application of the PSD.....	78
Table 19: Information that must be provided prior to Entering into a Framework Contract or Offer.....	91
Table 20: Examples of the National Application of the Payment Services Directive.....	106
Table 21: Key.....	114
Table 22: Core Acts in Force in Each SADC Country.....	117
Table 23: Acts of General Application in Force in Each SADC Country.....	118
Table 24: Comparing the Structure and Content of the National Payment System Act in South Africa, Namibia and Lesotho.....	121
Table 25: Comparing the Structure of the National Payment System Act and Regulations in Zimbabwe, Botswana, Seychelles and Swaziland.....	123
Table 26: Structure and Content of the Angolan and Mozambican National Payment System Acts.....	126
Table 27: Structure of the Zambian National Payment Systems Act, 2007.....	129
Table 28: Structure of the Malawian National Payment Systems Bill, 2014.....	131

Table 29: Structure of the DRC’s Draft Law on the Provisions Applicable to the NPS	133
Table 30: Key Definitions Contained in NPS Act and Subsidiary Legislation.....	139
Table 31: Terms Defined in the Settlement Finality Directive 98/26/EC	144
Table 32: Terms Defined in Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions.....	145
Table 33: Terms Defined in Directive 2007/64/EC Payment Services in the Internal Market (PSD).....	145
Table 34: Terms Defined in Regulation (EC) No 924/2009 Cross-border Payments in the Community.....	146
Table 35: Terms Defined in Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro.....	147
Table 36: Comparative Review: Powers and Functions of the Central Bank NPS Act / Bill	154
Table 37: Gap Analysis and Comparative Review: Confidentiality, Disclosure and Indemnity	163
Table 38: Public Interest Objective Provisions found in Law n° 2/2008	165
Table 39: Criteria for Access and Participation in NISS	175
Table 40: Documents to be provided by NBFIs Applying for Designation	176
Table 41: PFMI’s 8 and 9	178
Table 42: Number of Countries Defining the Moment of Opening of Insolvency Proceedings.....	191
Table 43: Prohibition of Payment Intermediation found in the Domestic NPS Act	203
Table 44: Domestic Dispute Resolution Provisions in National Payment System Acts / Bills	205
Table 45: International Dispute Resolution Mechanism.....	207
Table 46: Criteria for Accreditation of Authentication Products and Services	214
Table 47: Information to be provided to Consumers.....	215
Table 48: International and Regional Best Practice Electronic Communications and Transactions.....	217
Table 49: Level of Development of E-Money Regulatory Frameworks in SADC Member States	222
Table 50: Types of E-Money Accounts.....	224
Table 51: Suspension and Cancellation of Authorisation.....	225
Table 52: Specific Requirements for Issuing E-Money in Namibia	226
Table 53: Transaction Limits	228
Table 54: Fees Payable by E-Money Issuers	228
Table 55: Initial and Ongoing Capital Requirements.....	228
Table 56: Level of Compliance with Best Practice (E-Money).....	230
Table 57: Provisions on Payment Services	237
Table 58: Transparency Conditions and Information Requirements	241

Table 59: Rights and Obligations in Relation to the Provision of Payment Services.....	244
Table 60: Compliance with Component A FATF Recommendation 10: When is CDD required?	251
Table 61: Thresholds Applied (Occasional Transactions)	260
Table 62: Required CDD Information	263
Table 63: Documents Listed	267
Table 64: Independent Verification Sources Listed	270
Table 65: Timing and Verification of Identity	277
Table 66: Risk Based Approach Mandated in Law or Regulation	281
Table 67: Exemptions or Simplified CDD in Law or Regulation.....	286
Table 68: Compliance with FATF Recommendation 11 – Record Keeping.....	298
Table 69: Compliance with FATF Recommendation 13 – Correspondent Banking.....	304
Table 70: Compliance with Recommendation 15.....	309
Table 71: Compliance with FATF Recommendation 16	316
Table 72: Compliance with FATF Recommendation 17	322
Table 73: Examples of Attempted Transactions.....	326
Table 74: Indicators of Suspicious and Unusual Transactions	328
Table 75: Compliance with FATF Recommendation 20: Suspicious Transaction Reporting	331
Table 76: Compliance with FATF Recommendation 34 Guidance and Feedback	336
Table O1: Content of Irish S.I. No. 539/1998.....	345
Table P1: Section 7 of the Electronic Communications Act 2000	348
Table P2: Content of United Kingdom Electronic Signatures Regulation 2002.....	349
Table Q1: European Communities (Electronic Money) Regulations 2011	353
Table R1: Financial Service (EEA) (Payment Services) Regulations, 2010.....	368

DIAGRAMS

Diagram 1: SADC Institutional Framework.....	6
Diagram 2: Risk-Based Approach (The Exemptions).....	36
Diagram 3: Customer Due Diligence Requirements for “Standard” Customers	41
Diagram 4: European Union – Evolution of a Common Regulatory Framework for Payments	51
Diagram 5: Content of Title II.....	80
Diagram 6: Content of Title III	88
Diagram 7: Content of Title IV.....	96
Diagram 8: Content of Title V	106
Diagram 9: Strong Legal Influence (Similar Acts).....	120
Diagram 10: Scope of a “Sound Legal Basis”	137

EXECUTIVE SUMMARY

The SADC Payment System Integration Project and the SADC Integrated Regional Electronic Settlement System (SIRESS)

At its meeting held in Pretoria in May 2009, the Committee of Central Bank Governors (CCBG) of the Southern African Development Community (SADC), granted approval for the initiation of the SADC Payment System Integration project. At the core of this project is the testing of the SADC Integrated Regional Electronic Settlement System (SIRESS) in the four Common Monetary Area (CMA) countries.

The SIRESS Proof of Concept (POC) in the CMA went live on the 22 July 2013 and the second phase, opening participation to the system to some of the non-CMA SADC countries, commenced in October 2013. During the proof of concept phase of the project, the South African Reserve Bank is hosting and operating SIRESS. All participants in the settlement system are required to have accounts in SIRESS as ordinary members. The South African Reserve Bank is, on behalf of the SIRESS participating Central Banks, therefore the operator of the system and at the same time is also a participant.

SADC Payment System Integration Project seeks to replicate the achievements in Europe to date. This will require a harmonised legal and regulatory framework

The SADC Payment System Integration project, to a large extent, seeks to replicate the achievements in Europe. Key to the establishment of an integrated payments market in the European Union (EU) was the development of a single market which has been under construction in the EU since 1973. Since 1998 a number of binding legal instruments pertaining to payments, have been adopted in the EU. These include both regulations and directives. Three regulations pertaining directly to payment systems have been passed since 2001. These cover cross-border payments in Euro, information on the payer accompanying transfers of funds and technical and business requirements for credit transfers and direct debits in Euro. Regulation 2560/2001 which was later repealed by Regulation 924/2009 is widely recognised as the foundation of SEPA.

Over time, the EU legislature's focus has broadened to cover various, increasingly complex aspects of payment and securities systems with the adoption of the following directives: the Settlement Finality in Payment and Securities Settlement Systems (Directive 98/26/EC) as amended by Directive 2009/44/EC; the Community Framework for Electronic Signatures (Directive 1999/93/EC); the Taking-up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions (Directive 2009/110/EC) which repealed Directive 2000/46/EC; Directive 2002/47/EC on financial collateral arrangements as amended by Directive 2009/44/EC; Directive 2004/39/EC on markets in financial instruments, which replaced Directive 93/22/EC on investment services in the specified securities field.

There is no harmonised legal and regulatory framework for payments in SADC

At present, a harmonised legal and regulatory framework for payments does not exist in SADC and the region also faces a number of institutional challenges. The SADC Central Bank is yet to be established and SADC does not have a Parliament with legislative powers as in other similar regions such as the East African Community (EAC), EU and the Economic Community Of West African States (ECOWAS). There are no SADC Regulations and or Directives on Payments (Annex 6 of the Finance and Investment Protocol however establishes a framework for cooperation and

coordination between Central Banks on payment, clearing and settlement systems) and the SADC Tribunal remains disbanded.

Multilateral agreements provide a short term solution

SADC Member States participating in the SIRESS POC project have elected to structure the legal arrangements between participants through a number of multilateral agreements. These agreements have been drafted as a short term solution in order to provide for legal certainty until such time as an appropriate SADC wide legal and regulatory framework has been developed and adopted. Over the longer term, all fourteen SADC countries are committed to harmonising their legal and regulatory frameworks and to establishing the institutional and organisational structures conducive to the establishment of an integrated payments market.

The drafting of a model payment system law the most appropriate option at this time

The harmonisation of payment system law in SADC will, in the most part depend on Member States being willing to amend their domestic law in line with the Payment System Model Law proposed. While the legal basis for the harmonisation of Payment System Law in the SADC region is found in the Annex 6 of the Protocol on Finance and Investment (FIP), unlike Article 2 of Annex 5 of the FIP that requires State Parties to “promote the mutual co-operation, co-ordination and harmonisation of the legal and operational frameworks of Central Banks which shall culminate in the creation of a Model Central Bank Statute for the Region as contemplated by the [Regional Indicative Strategic Development Plan] RISDP” article 6(1)(c) of Annex 6 does not require the creation of a Payment System Law. Instead, the article states simply that, “the SADC Payment System Steering Committee shall consider and recommend the enactment of, or amendments to, legislation of State Parties relating to payment systems, clearing systems and settlement systems, including the making and amendment of rules and procedures, risk management policies and any other matters relevant to such legislation and such payment systems, clearing systems and settlement systems.”

Given the current institutional structure of SADC, the lack of consensus on whether the Summit or the Council has the power (as is the case in the EU), to promulgate binding regulations that would have force of law in each SADC Member State without the need for any act of acceptance or incorporation into the domestic, it appears that the only option at this time is to propose the drafting of a Payment System Model Law. Such a Model Law must have the status of soft law to inform policy making in each SADC Member State. As such, it must be developed under the auspices of one of the SADC structures fully mandated to do so by the SADC Treaty. It is also important to take into account current differences in legal traditions, regulatory models and different levels of infrastructural development.

International Best Practice: The Choice of Soft Law Benchmarks

Article 4(1)(e) of Annex 6 to the FIP requires each Member State to “monitor, on an ongoing basis, international payment system best practices and align the payment system developments in that State Party in accordance therewith.” Within the payments field, several documents published by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS), the Basle Committee and the Financial Action Task Force (FATF) are recognised as sources of international best practice. The following soft laws were chosen as best practice benchmarks:

- [Principles for Financial Market Infrastructures \(PFMIs\)](#);²
- [United Nations Commission on International Trade Law \(UNCITRAL\) Model Law on Electronic Commerce \(1996\)](#);
- [FATF Recommendations \(2012\)](#);³
- [The Bank for International Settlements \(BIS\) / World Bank General Principles for International Remittance Services](#).⁴

International Best Practice: The Choice of Hard Law Benchmarks

The SIRESS project is modelled on the Single Euro Payments Area (SEPA). Consequently, the regulatory framework adopted by the EU serves as an appropriate benchmark when considering the harmonisation of payment, clearing and settlement system laws and regulations in the SADC region.

[Regulation \(EC\) No 924/2009 Cross Border Payments in the Community](#)

This Regulation lays down the rules for cross-border payments in the community and ensures that charges for cross-border payments within the Community are the same as those for payments in the same currency within a Member State. In light of the introduction of SIRESS and with additional payment streams being added over time, the CCBG and the SADC Payment System Steering Committee will need to determine how cross-border issues such as charges for cross-border payments and corresponding national payments, measures for facilitating the automation of payments, balance of payments reporting obligations, interchange fees for cross border direct debit transactions and the reachability of direct debit transactions will be regulated. The ideal solution would be for the appropriate SADC institution (the Senate) to issue a binding Regulation covering these matters.

[Regulation \(EC\) No. 178/2006 Information on the Payer Accompanying Transfer of Funds](#)

This regulation lays down the rules for payment service providers to send information on the payer throughout the payment chain. This is done for the purposes of prevention, investigation and detection of money laundering. The requirements set out in the Regulation have synergies with FATF Recommendation 16.

[Regulation \(EU\) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in EURO](#)

This Regulation lays down the rules for credit transfer and direct debit transactions denominated in Euro within the EU where both the payer's payment service provider and the payee's payment service provider are located within the EU, or where the sole payment service provider involved in the payment transaction is located in the EU. The subject matter covered includes the reachability of Payment Service Providers (PSPs), interoperability, end dates, the validity of mandates and the right to a refund, interchange fees for direct debit transactions, payment accessibility, the designation of competent authorities, penalties and out-of-court complaint redress mechanisms. In light of the introduction of SIRESS and with additional payment streams being added over time and the move towards a single currency and customs union, the

² Bank for International Settlements and International Organization of Securities Commissions 2012 *Principles for Financial Market Infrastructures*.

³ Financial Action Task Force 2012 *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The Recommendations*.

⁴ Bank for International Settlements and The World Bank 2007 *General Principles for International Remittance Services*.

CCBG and the SADC Payment System Steering Committee will need to determine how all these issues will be regulated in a harmonised fashion.

[Directive 98/26/EC Settlement Finality in Payment and Securities Settlement Systems](#)

Directive 98/26/EC Settlement Finality in Payment and Securities Settlement Systems was adopted in May 1998. As noted in the Commission of the European Communities, Directive 98/26/EC was the “Community legislator’s response to the concerns identified by the Committee on Payment and Securities Systems (CPSS) under the auspices of the Bank for International Settlements regarding systemic risk. With the start of stage II of the Economic and Monetary Union (EMU) in 1994, it became evident that there was a need for a stable and efficient payment infrastructure to assist cross-border payments, to support the future single monetary policy and to minimise systemic risk especially in view of the increasing cross-border aspects.”⁵ Directive 98/26/EC aimed to reduce the systemic risk associated with participation in payment and securities settlement systems, and in particular the risk linked to the insolvency of a participant in such a system. As noted on the European Commission website, Directive 98/26/CE aims to “contributes to the efficient and cost-effective operation of cross-border payment and securities settlement arrangements, thereby reinforcing the freedom of movement of capital and the freedom to provide services within the internal market.”⁶

The substantive provisions contained in this Directive are used throughout the report as a best practice benchmark against which the provisions on transfer orders and netting, provisions concerning insolvency and collateral security are measured.

[Directive 2009/110/EC on the Taking Up, Pursuit & Prudential Supervision of the Business of Electronic Money Issuers](#)

Directive 2000/46/EC on Electronic Money Institutions was repealed by Directive 2009/110/EC E-Money. The new E-Money Directive aims to enable new, innovative and secure electronic money services to be designed, to provide market access to new companies and to foster real and effective competition between all market participants.

The substantive provisions contained in this Directive are used through the report as a best practice benchmark against which the provisions contained in legally enforceable Directives and the non-enforceable E-Money Guidelines applicable in SADC Member States are measured.

[Directive 2007/64/EC Payment Services in the Internal Market \(PSD\)](#)

Directive 2007/64/EC on Payment Services in the Internal Market (The PSD) provides the necessary legal platform for SEPA and is known as the new legal framework for payments (NLF). The aim of the directive is to harmonise legislation pertaining to the provision of payments services within the EU, increase competition, reinforce consumer protection through transparency of information and charges and define the rights and obligations of payment service providers and their users. The PSD became law on 1 November 2009 and ensures that the rules on electronic payments are the same in 30 European countries (EU, Iceland, Norway and Liechtenstein). Transposition of the PSD into national legislation was mandated, allowing Member States limited discretion during implementation. Each EU member state has the right

⁵ Commission of the European Communities 2006 *Evaluation Report on the Settlement Finality Directive 98/26/EC* (EU 25) Brussels 3.

⁶ See http://ec.europa.eu/internal_market/financial-markets/settlement/dir-98-26-summary_en.htm

to assign whichever regulator or competent authority it defines as the most appropriate to oversee the implementation of the PSD and ensure a successful introduction of the PSD principles into operational practices at the national level.

The substantive provisions contained in this Directive are used through the report as a best practice benchmark against which provisions found in laws and regulations applicable in SADC Member States are measured.

A Sound Legal Basis

Principle 1 of the Principles for Financial Markets Infrastructures (PFMI's) requires that FMIs should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of their activities in all relevant jurisdictions. Paragraph 3.1.2 of the *Principles for Financial Market Infrastructures (PFMI)* report reads as follows: "The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions. The legal basis consists of the legal framework and the FMI's rules, procedures, and contracts. The legal framework includes general laws and regulations that govern, among other things, property, contracts, insolvency, corporations, securities, banking, secured interests, and liability. In some cases, the legal framework that governs competition and consumer and investor protection may also be relevant. Laws and regulations specific to an FMI's activities include those governing its authorisation and its regulation, supervision, and oversight; rights and interests in financial instruments; settlement finality; netting; immobilisation and dematerialisation of securities; arrangements for Delivery versus Payment (DvP), Payment versus Payment (PvP), or Delivery versus Delivery (DvD); collateral arrangements (including margin arrangements); default procedures; and the resolution of an FMI."⁷

Broken down further, a country's laws and regulations should, at the minimum provide for the following:

- regulation and oversight by the Central Bank;
- settlement provisions;
- netting arrangements;
- the establishment of the official currency backed by the Central Bank;
- provisions governing the issuance, acceptance and negotiation of cheques;
- laws and regulations paper-based credit transfers and electronic wire transfers;
- laws and regulations governing the rights and obligations of card issuers, cardholders and merchants;
- laws and regulations governing the issuance and use of E-Money;
- laws and regulations governing payment services;
- laws and regulations governing the payments leg of securities transactions;
- electronic communications and transactions laws and regulations;
- Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws and regulations;
- competition laws and regulations;
- consumer protection laws and regulations.

⁷ Bank for International Settlements and International Organization of Securities Commissions 2012 *Principles for Financial Market Infrastructures* 23.

[Overarching Gap Analysis \(Current Laws and Regulations in SADC Member States\)](#)

Section 4.2 of this report provides a high-level gap analysis highlighting legislation (Acts) and regulations that are legally enforceable in each SADC Member State, draft bills and bills that have been drafted but are not legally enforceable, as they have not been tabled in Parliament or assented to and signed. Where no legally enforceable law or regulation is in place, this gap is highlighted. For the purposes of this study, laws and regulations are divided into “core” and “general application” laws and regulations. Core laws and regulations refer to those instruments that have a direct bearing upon the activities of FMI’s. This group of core laws and regulations consists of: 1) the Central Bank Act, 2) the Bank Act, 3) the Financial Institutions Act, 4) the National Payment System Act, 5) Bills of Exchange Act, 6) Electronic Money Act, 7) Payment Services Act, 8) Securities Act, 9) Stock Exchange Act, 10) CSD Act, 11) Exchange Control Act, 12) Electronic Communications and Transmissions Act, 13) Anti-Money Laundering (AML) Act, 14) Countering the Financing of Terrorism (CFT) Act and 15) the Financial Intelligence Centre (FIC) Act. In several countries, the AML, CFT and FIC Acts are amalgamated into one general AML Act or FIC Act.

The laws of general applicability relevant to the analysis in the report are: 1) the Company Act, 2) Competition Act, 3) Insolvency Act, 4) Access to Information Act, and 5) the Consumer Protection Act.

SADC Member States are at different stages of development of their legal and regulatory frameworks for payments. For the purposes of this project, the primary gap highlighted is that the DRC, Lesotho, Malawi and Tanzania do not have a legally enforceable National Payment System Act in place. All four of these countries are at varying stages of the legislative process with respect to having their Bills tabled and promulgated. Mauritius is the only country that has not drafted a National Payment System Bill. All five of these countries are therefore exposed in terms of there being no legally enforceable law in place governing vital issues such as insulation of collateral security from the effects of insolvency, settlement finality and irrevocability, Central Bank oversight and supervision of the National Payment System. Some of these provisions are contained in settlement system and Automated Clearing House (ACH) Rules, Terms and Conditions and Policies and Procedures, however, it preferable that these provisions are set down in law and not in bi-lateral agreements or in legally unenforceable documents. In Mauritius for example, provisions on settlement finality and irrevocability and money settlements in central bank money are not included in Mauritian Law or Regulations. This should be an area of concern as the only references to finality and irrevocability are found in the Port Louis Automated Clearing House Rules and the Mauritius Automated Clearing and Settlement System Terms and Conditions. The reliance on these bi-lateral arrangements between participants’ results in an ad-hoc self-regulated payments industry, a situation that should not be left unchecked by the Central Bank. As the payment systems are maturing in the DRC, Lesotho, Malawi, Tanzania and Mauritius, it is vital that the Bills that have, in some cases been outstanding for more than ten years, are passed. In the case of Mauritius, legislation in the form of a National Payment System Act should be introduced as soon as is reasonably practicable, so as to allow for more formalised regulation.

The formal regulation of electronic money (E-Money) and payment services is poor in all 14 SADC Member States. Only two countries, the DRC and Namibia have issued a legally enforceable determination (Namibia) and directive (DRC) on the matter. Most SADC Member States do not have a well-structured legal and regulatory framework for retail payments. In all 14 SADC countries, vital issues such as card payments, agent banking, the authorisation of payment service providers, the issuance of payment instruments and the rights and obligations of PSPs and users are, in the most part, set out in guidance notes, guidelines and position papers. These by their very nature are not legally enforceable.

In recognition of the growing importance of retail payments and the need to harmonise domestic law in this area, the European Parliament and the Council adopted Directive 2007/64/EC Payment Services in the Internal Market (PSD) otherwise known as the Payment Services Directive in November 2007. Member States had until 1 November 2009 to transpose the Directive into National Law. None of the fourteen SADC Member States have such a law in place, although some of the provisions found in the PSD have been included in the DRC's Draft Law on the Provisions Applicable to the National Payment System.

Another area of concern is the fact that only four countries have promulgated a separate Electronic Communications and Transmissions Act. While some provisions on the *prima facie* nature of electronic documents have been included in the National Payment System Act in several countries, vital provisions on for example, evidentiary proof of authentication of electronic payments using digital signatures or other instruments for electronic payment authorisation, the establishment and maintenance of a register of cryptography providers and the accreditation of authentication products and services in support of advanced electronic signatures by a recognised Accreditation Authority are not covered by law and regulation.

Only two of the fourteen SADC Member States have a stand-alone Central Securities Depository Act. In general, the issue of the regulation of the payments leg of securities transactions is not well covered in law and regulation. Mozambique and Angola are the only two SADC Member States that include a provision on the finality and irrevocability of securities settlements in their National Payment System Acts.

All fourteen SADC Member States have comprehensive AML/CFT legal and regulatory frameworks in place. Several countries have elected to promulgate one Act that covers AML, CFT and the operations of a Financial Intelligence Centre. Others, such as Namibia and South Africa have split these matters into three different statutory instruments.

Regional Grouping 1

Similar National Payment System Acts: South Africa,

The review of the National Payment System Act / Payment System Management Act or Bill in each SADC country has shown a certain level of harmonisation in specific groupings of countries. The structure of the National Payment System Act in South Africa, Namibia and Lesotho are similar. The Namibia Payment System Management Act, 2003 (As Amended)⁸ however contains two provisions that are not found in the

⁸ Act 18 of 2003 (As Amended).

Namibia and Lesotho (Bill)

South African National Payments System Act, 1998 (As Amended)⁹, namely, indemnity (Section 12) and the power of the Bank to, by notice in the Gazette, make determinations not inconsistent with the Act (Section 14). Determinations are not defined in the Namibian Payment System Management, 2003 (As Amended) but have the same force of law as Regulations. Several provisions in Lesotho's Payment Systems Bill, 2013 have been influenced by the South African Act, particularly the provisions relating to the Payment System Management Body. However, this Bill appears to also contain provisions found in other Act in force in the Region. An example of this are Section 26 on the admissibility of electronic and optical evidence, a provision not found in South Africa or Namibia's National Payment System Acts. Lesotho is also the only country in the SADC Region that has elected to make use of a licensing regime instead of the typical designation or recognition approach. The Bill does not refer to "designation" or recognition of systems. Instead, Section 9 reads, "a person shall not operate a system in Lesotho, unless the person is in the possession of a licence for this purpose, obtained from the Central Bank." Lesotho's Bill contains dedicated Parts on insolvency (Part V) and collateral arrangements (Part VI), but does not, unlike the South African and Namibian Acts respectively; contain provisions on confidentiality, indemnity, the settlement of disputes, and the retention of records or application for a court order.

Regional Grouping 2**Similar National Payment System Acts: Angola and Mozambique**

The Angolan and Mozambican Acts are similar in both structure and content. This is not surprising given the similar legal systems in both countries and the use of the Portuguese language. Both the Angolan and Mozambican Acts contain a specific Article on public interest objectives. While the "public interest" is mentioned in several other National Payment System Acts in the SADC region, the Angolan and Mozambican Acts are the only two Acts that specifically list security, reliability, transparency and efficiency as public interest objectives. The Mozambican Act also contains several unique provisions not found in the Angolan Act. Article 10 of the Mozambican Law n° 2/2008 for example, establishes the National Payment System Coordinating Committee (CCSNP). This Committee is chaired by the *Banco de Moçambique* and includes representatives from: the *Banco de Moçambique*; Ministry of Finance; National Communications Institute; Mozambican Securities Exchange; Mozambican Bankers' Association; Commercial banks and Companies providing payment services. The powers and functions of the CCSNP is set out in Article 11. Article 17 on Payment Instruments, Transactions and Electronic Archives that is included in the Mozambican Law is not included in the Angolan Law. Article 24 of the Mozambican Act covers Settlement of Operations with Truncation and Article 24(1) states that "Truncation of cheques and other instruments is permitted, up to the value and under the conditions defined by the *Banco de Moçambique* upon the recommendation of the National Payment System Coordinating Committee." The Mozambican Act also includes a provision on Delivery Versus Payment (DVP), a provision not found in any other National Payment System Acts in the SADC Region.

Regional Grouping 3

The influence of Zimbabwe's National Payment System Act, 2001¹⁰ is clearly evident in Botswana's National Clearance and Settlement System Act, 2003¹¹ the Seychelles

⁹ Act 78 of 1998 (As Amended).

¹⁰ [Chapter 24:23].

¹¹ Act 5 of 2003.

Almost Identical National Payment System Acts: Zimbabwe, Botswana, Seychelles and Swaziland

National Clearing and Settlement System Act, 2010¹² and Swaziland's National Clearing and Settlement Systems Act, 2011.¹³ It appears that structure and substantive content of Zimbabwe's National Payment Systems Act [Chapter 24:23] was used by Botswana, Seychelles and Swaziland as the template for their domestic law as the provisions are almost identical. Botswana, Seychelles and Swaziland have however improved on the original content of Zimbabwe's National Payment Systems Act [Chapter 24:23], added additional sections and incorporated several domestic nuances. Botswana for example, included specific provisions not found in the Zimbabwean Act on: unpaid items due to insufficient funds (Section 23), computer entries (Section 24), imaging (Section 25) and the Ministers power to make regulations providing for the better carrying out of the provisions of the Act (Section 27). The Seychelles National Clearance and Settlement Systems Act, 2010¹⁴ contains a provision on record keeping not found in the Zimbabwean, Botswana or Swaziland Acts. Seychelles has also derogated from the Zimbabwe and Botswana Acts through the insertion of sections 11(1) and 11(2) into the Seychelles National Clearance and Settlement Systems Act, 2010.

Swaziland also appears to have drawn heavily upon the Botswana National Clearance and Settlement Systems Act, 2003¹⁵ as a template as the Swaziland National Clearing and Settlement Systems Act, 2011¹⁶ more closely resembles that Botswana Act than the Zimbabwean Act. Seychelles appears to have used the Botswana National Clearance and Settlement Systems Act, 2003 as the template for their National Clearance and Settlement Systems Act, 2010 as the structure and content of the Seychelles National Clearance and Settlement Systems, 2010 more closely resembles the Botswana Act than the Zimbabwe Act.

The Bank of Botswana, in recognition of the fact that the National Clearance and Settlement System Act, 2003¹⁷ did not cover several important provisions, issued the National Clearance and Settlement Systems Regulations, 2005, to rectify some of these gaps. Botswana's Regulations cover *inter alia*: application for a certificate of recognition (Regulation 3), conditions for recognition (Regulation 4), investigation of unrecognised systems (Regulation 7), rules and procedures of management bodies (Regulation 14), and offences and penalties (Regulation 18).

Regional Grouping 4

Unique Acts: DRC (Draft Law), Malawi (Bill) and Zambia's National Payment Systems Act, 2007

Malawi's National Payment Systems Bill, 2014 is clearly and logically structured and contains nine parts and forty-four sections. The powers and functions of the Reserve Bank in relation to payment, clearing and settlement systems are clearly set out in Part II. PART III is a stand-alone part on the regulation and oversight role of the Central Bank. This Bill is a good example of a "Newer Generation Act" as it's extends well beyond the "designation or recognition of clearing and settlement systems" and the regulation and oversight thereof, as is the case in most other National Payment System Acts.

¹² Act 12 of 2010.

¹³ Act 17 of 2011.

¹⁴ Act 12 of 2010.

¹⁵ Act 5 of 2003.

¹⁶ Act 17 of 2011.

¹⁷ Act 5 of 2003.

Section 3(1) of the National Payment Systems Bill, 2014 is unusual in that it states that, “the principle objective of this Act is to provide for the regulation and oversight of payment, clearing and settlement systems, payment instruments, remittance service providers, electronic money transfers, card issuers, travellers cheques agencies by – (a) promoting the soundness, integrity, safety and efficiency and reliability of the payment, clearing and settlement systems or payment instruments including security and operating standards, and infrastructure arrangements; (b) providing for minimum standards for protection of customers; and (c) determining respective rights and obligations of system operators, participants and customers.”

This Section extends the ambit of the regulation and oversight of the Reserve Bank from simply looking at systemically important payment systems (SIPS) into the retail payments domain.

Additionally, Section 12(1) of the National Payment Systems Bill, 2014 prohibits a person from establishing or operating any payment, clearing and settlement system or services, remittance services including electronic money transfer services, mobile payment services or issuing payment instruments without a licence or prior authorisation from the Reserve Bank from the Reserve Bank of Malawi.

Zambia’s National Payment Systems Act, 2007¹⁸ contains several unique provisions on “payment system businesses.” In terms of Section 11, the Bank of Zambia is mandated to regulate and oversee the operations of payment systems businesses to ensure the efficiency, integrity, effectiveness, competitiveness and security of the payment system so as to promote the safety and stability of the Zambian financial system. Section 12(1) requires a person intending to conduct, or offer to conduct, any payment system business to apply for designation by the Bank of Zambia. Section 13 prohibits a person from conducting a payment system business as an intermediary unless the person is, (a) a participant, (b) designated as a payment system business under section 12 or (c), exempted by the Bank of Zambia under the Act. These provisions are particularly relevant in light of the requirements set out in the BIS/World Bank General Principles for International Remittance Services report (2007). An additional feature of the Zambian National Payment Systems Act, 2007 is the inclusion of provisions on the electronic presentment of cheques. Part IV of the Zambian National Payment Systems Act, 2007 overrides the provisions in the Bills of Exchange Act, 1882 where applicable. Section 15(1) reads, “subject to subsection (3), a banker may present a cheque for payment to a banker, on whom it is drawn, by electronically transmitting it by other means instead of presenting the cheque itself.” In terms of Section 15(2), where a cheque is presented for payment, under subsection (1), physical presentment at the premises of the drawee’s bank at a reasonable hour of a working day is no longer necessary. Section 15(1) empowers the Bank of Zambia to prescribe the physical features of a cheque.

The DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 is the longest Act in the region (108 Articles). The Draft Law contains detailed

¹⁸ Act 1 of 2007.

provisions on payment instruments, access to financial services, interoperability, the obligations of payment service providers, issuer obligations, holder obligations, E-Money, evidence and electronic signatures and the monitoring of payment systems and payment instruments. The DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 appears to directly incorporate several provisions from Directive 2007/64/EC Payment Services in the Internal Market (PSD) and combine these with provisions found in "conventional" National Payment System Acts.

Substantive Content of Law

Definitions

A section containing definitions of various words or phrases used in an Act and or Subsidiary Legislation (Regulations, Determinations, and Directives) is usually near the beginning of the Act. The headings of such sections vary. Some SADC countries use the word 'Interpretation', others 'Definitions' others 'Terms used'. Occasionally, as is the case in the Mozambican Law n° 2/2008 of 27 February, definitions are contained in a 'Glossary' at the back of an Act. On several occasions during the research phase of this project, the need for a common understanding of key payment related terms by SADC Regulators has been identified. The lack of a common standard can lead to legal uncertainty and general confusion when, for example, terms such as E-Money have vastly different meanings in each SADC Member State. This problem has been resolved in the EU through the passing of Regulations and Directives, promulgated either jointly by the EU Council and European Parliament, or by the Commission alone, that contain set definitions which are adopted automatically by Member States in the case of Regulations and incorporated into domestic laws and regulations by Member States in the case of Directives.

There is currently no term or definition that is commonly defined by every SADC Member State.

Substantive Content of Law

Powers and Functions of the Central Bank with respect to the National Payment System as set out in the Central Bank Act

In addition to the powers and function of each Central Bank with respect to the regulation and oversight of the National Payment System as set out in the primary National Payment System Act, all fourteen Central Banks also derive their mandate from provisions contained in the Central Bank Act. The proposed benchmark in this regard is section 10(1)(c)(i) of the South African Reserve Bank Act, 1989 (As Amended)¹⁹ which provides that the South African Reserve Bank may "perform such functions, implement such rules and procedures and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems." It is important to note that reference is made to payment, clearing and settlement systems, leaving the scope wide enough to include both systemically important and non-systemically important payment systems. When provisions contained in other Central Bank Acts are compared against the provision in the South African Reserve Bank Act, 1989 (As Amended) it is clear that most provisions fall short in a number of respects.

Substantive Content of Law

It is important to acknowledge that different countries apply different approaches (this is particularly so with respect to the authorisation, licensing, designation, or

¹⁹ Act 90 of 1989 (As Amended).

[Powers and Functions of the Central Bank with respect to the National Payment System as set out in the National Payment System Act or Bill](#)

recognition of payment systems, payment system operators, participants and instruments), but at the same time, there is a need to standardise and harmonise the approach taken in the SADC region. An example of a harmonised approach is found in Articles 6 and 10 of the Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC) that requires Member States to notify to the Commission of which systems and respective system operators they have designated and which national authorities are in charge of notification. The Commission holds two registers with this information. They are up-dated whenever Member States send new information to the Commission. Article 10(1) reads: "Member States shall specify the systems, and the respective system operators, which are to be included in the scope of this Directive and shall notify them to the Commission and inform the Commission of the authorities they have chosen in accordance with Article 6(2). The system operator shall indicate to the Member State whose law is applicable the participants in the system, including any possible indirect participants, as well as any change in them. In addition to the indication provided for in the second subparagraph, Member States may impose supervision or authorisation requirements on systems which fall under their jurisdiction. An institution shall, on request, inform anyone with a legitimate interest of the systems in which it participates and provide information about the main rules governing the functioning of those systems."

Where a country has elected not to empower the Central Bank, together with licensed banking institutions to form a juristic person (Payment System Management Body) and to confer certain powers and functions on the juristic body, it should follow that these powers and functions should remain with the Central Bank and be reflected in the National Payment System Act accordingly. It is however evident from the analysis presented in this report and individual country reports that several Acts have substantial gaps and many of the powers and functions that should be conferred on the Central Bank by the National Payment System Act, are not.

Areas of particular concern include: the lack of specific oversight provisions in several Acts; the specific mandate for the Central bank to operate a settlement system and participate in such a system; very few provisions on allowable sponsorship arrangements; few provisions on payment service providers and even fewer provisions on payment instruments. Several Acts contain no provisions on inspections and investigations. Perhaps the most glaring gap in several Acts is the lack of provisions pertaining to the power to issue Regulations, Directives and Guidelines and to impose administrative sanctions. It is also particularly alarming that only three SADC Member States have provisions in their Acts requiring the Central Bank to cooperate with other domestic regulatory authorities and international regulatory authorities.

Substantive Content of Law

[Public Interest Objectives](#)

Most National Payment System Acts in force in SADC Member States make reference to the "public interest" several times without defining what the "public interest" is. For example, Section 15(2)(b) of Lesotho's Payment Systems Bill, 2013 requires the Governor to, in considering whether or not to issue a directive in terms of section 15(1) to have regard to whether reasonable grounds exist to believe that any person is engaging in or is about to engage in any act, omission or course of conduct, with respect to the payment system that is likely to be contrary to the public interest.

In contrast to the general public interest statements found in most National Payment System Acts in force in SADC Member States, two countries in the SADC region, namely Angola and Mozambique include specific public interest objectives in their National Payment System Act. Should all fourteen SADC countries elect to draft a Model Payment System Act, it is strongly recommended that the “public interest” is defined and that a provision such as the Mozambican provision be included in the model law. In addition to the five articles found in the Mozambican law, provisions covering *inter alia*: co-operation and competition and consumer protection should be considered.

Substantive Content of Law

[Access to Clearing and Settlement Systems](#)

One of the key findings set out in the South African Banking Enquiry Report to the South African Competition Commission was that, “the existing regulatory regime for the National Payment System [in South Africa] does not appear to meet the needs of South African consumers for competitive and technically innovative payment services. The approach of largely ignoring non-bank activities has begun to shift. But persistence in the view that only clearing banks may participate in clearing and settlement is not an approach that will best serve South Africa’s interest. We are convinced of the need for a revision of the regulatory approach and the development of an appropriate regulatory regime for payment system activity which is functionality-based, rather than institutionally based, so as to ensure quality of access regardless of whether they are clearing banks or not.”²⁰

In most SADC Member States, access to clearing and settlement systems remains the exclusive domain of the Central Bank and Banks. Several Central Banks while mandated by the National Payment System Act to set access and participation criteria have not done so. In several cases, the domestic law is unclear on who has access to and may participate in the settlement system or clearinghouse. In other cases such as in Botswana, the provisions of the Law seem to be at odds with the stance taken by the Bank of Botswana that “membership of BISS is open to all clearing banks operating in Botswana as well as the Bank of Botswana” as section 3(3)(a) of the National Clearance and Settlement Systems Act, 2003²¹ refers to “financial institutions” in the broader sense and not simply to licensed banks. Several Acts are silent on permissible sponsorship arrangements. In the absence of a legally enforceable National Payment System Act, the DRC, Lesotho, Malawi, Mauritius and Tanzania rely on various agreements, rules and Terms and Conditions to regulate access and participation, a situation that is far from ideal. The current stance taken by South Africa and Namibia are good examples of how the thinking of a number of Central Banks with respect to allowing non-bank participation in the clearing and settlement domain is changing.

In terms of Strategic Objective 1 of Vision 2015, the South African Reserve Bank is committed to continuing to evaluate and improve the participation of non-bank stakeholders in the clearing system and/or in formal payment system management structures. It is important to note that the Vision 2015 document specifically lists six categories of potential participants in the National Payment System. These are:

²⁰ The Banking Enquiry 2008 *Report to the Competition Commissioner by the Enquiry Panel* 508.

²¹ Act 5 of 2003.

Registered banks in terms of the South African banking legislation; qualifying non-banks that, subject to the discretion of the Bank, are designated to be clearing participants in terms of section 6 of the National Payment System Act; sponsored banks and non-banks that are designated by the Bank; non-bank participants that include third-party service providers and system operators; non-banks that are allowed to issue payment instruments; non-banks that issue prepaid instruments. Six strategies for increasing access to the National Payment System are presented in Vision 2015. Of particular relevance to this project are strategy 2) allow non-banks access to the National Payment System via directives; strategy 4) enhance entry criteria and other regulatory requirements for participants; strategy 6) introduce designation for different levels of non-bank participation in the National Payment System; strategy 7) amend legislation to enhance formal participation where required; and strategy 8) conclude MOUs between the National Payment System Department (NPSD) and other sector specific regulators.

To date, Namibia is the only SADC Member State that has issued a legally binding Determination that sets out the criteria for authorisation and participation in clearing and settlement systems for both banks and non-bank participants. In line with Objective 2 of Namibia's National Payment System Vision 2015, namely that "the objective of this strategic focus area is to enable access to payment system, thereby promoting financial inclusion", section 8 of PSD-6 sets out the Bank of Namibia's position on designating non-bank financial institutions (NBFIs) for the purposes of participating in clearing and settlement systems. It is highly recommended that all of the other SADC Member States consider adopting the position that has been taken by the Bank of Namibia.

Substantive Content of Law

Settlement Finality and Irrevocability

Legal certainty as to the effectiveness of transfers of funds and securities is a prerequisite for establishing market confidence, fostering the protection of investors and limiting risk in the financial markets. Of particular relevance in the context of the legal protection of market infrastructures is the concept of settlement finality and irrevocability.²² Finality is important because when it occurs, as set out in the laws, regulations and rules applicable in each country, the obligations generated in the interbank payment, clearing and settlement process are discharged. Therefore, the credit, liquidity and systemic risks generated as part of this process cease to exist at this point in time. As a result, finality is the most important concept in the analysis of the credit, liquidity and systemic risks in payment and settlement systems.²³

Over the years, finality has increasingly been associated with the reduction of insolvency-related risks resulting from participation in payment, clearing and settlement systems. In recognition of this, in 1998 the European Union adopted the Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC). This Directive applies to systems designated by their national authorities as being covered by it and created an EU-wide legal framework to reduce systemic risk linked to payment, clearing and settlement systems and to protect systems and their participants against the adverse effects of insolvency proceedings opened against another system participant.

²² Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 144.

²³ 145.

Two of the principles set out in the *Principles for Financial Market Infrastructures (PFMI)*²⁴ report are particularly relevant in this regard. These are: Principle 8 Settlement Finality and Principle 9 Money Settlements. Principle 8 requires that an FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time. Principle 9 requires that an FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.

Several of the current National Payment System Acts in force in several SADC Member States do not contain a provision requiring that money settlements be effected in Central Bank Money. An additional area of concern is that provisions on settlement finality and irrevocability and money settlements in central bank money are not included in Mauritian Law or Regulations. This is an area of concern as the only references to finality and irrevocability are found in the Port Louis Automated Clearing House Rules and the Mauritius Automated Clearing and Settlement System Terms and Conditions. The reliance on these bi-lateral arrangements between participants' results in an ad-hoc self-regulated payments industry, a situation that should not be left unchecked by the Central Bank. As the payment system is maturing in Mauritius, it is vital that legislation in the form of a National Payment System Act is introduced so as to allow for more formalised regulation.²⁵ The same can be said for the DRC, Lesotho, Malawi and Tanzania that have yet to pass their National Payment System Bills.

Substantive Content of Law

The Settlement Finality Directive (As Amended) ensures that netting is legally enforceable and binding on third parties even in the event of insolvency proceedings and precludes the application of zero-hour rules.

Transfer Orders and Netting

Transfer Orders and Netting Are Legally Enforceable and Binding on Third Parties

Article 3(1) of the Settlement Finality Directive (As Amended) provides that, transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings. This shall apply even in the event of insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system who is not a participant. Where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor

²⁴ Bank for International Settlements and International Organization of Securities Commissions *Principles for Financial Market Infrastructures (PFMI)*.

²⁵ Volker W *Essential Guide to Payments An Overview of the Services, Regulation and Inner Workings of the South African National Payment System* (2013) 267.

should have been aware, of the opening of such proceedings.

When compared to the provisions found in the National Payment System Act or Bill in each SADC Member State, the domestic provisions are found to be lacking in a number of respects. Problem areas include no reference to transfer orders and netting in the National Payment System Act, the lack of clarity on the defined moment of “the opening of insolvency proceedings”, no reference to insolvency proceedings against a participant in interoperable systems or against the system operator of an interoperable system which is not a participant and no provisions on transfer orders entered into the system after the moment of opening of insolvency proceedings.

No Law, Regulation or Rule Will Result in the Unwinding of a Netting

Article 3(2) of the Settlement Finality Directive (As Amended) reads, “no law, regulation, rule or practice on the setting aside of contracts and transactions concluded before the moment of opening of insolvency proceedings, as defined in Article 6(1) shall lead to the unwinding of a netting.” The Angolan Law n° 05/05 Dated July 29, the DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 and the Mozambican Law 02/08 of 27 February do not contain a provision of this nature. Other National Payment System Acts, such as Botswana’s National Clearance and Settlement Systems Act, 2003²⁶ refer to specific laws which limits the scope of the provision. It is therefore suggested that specific laws are not named but rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered. Section 25 of the Zambian National Payment Systems Act, 2007²⁷ is drafted very broadly and refers to “any other law to the contrary.” This is in contrast to most National Payment System Acts in the region that refer specifically to the Insolvency Act, Financial Services Act of Company Act. The provision in the Zambian law is preferred.

Interoperable Systems

Article 3(4) of the Settlement Finality Directive (As Amended) provides that, “In the case of interoperable systems, each system determines in its own rules the moment of entry into its system, in such a way as to ensure, to the extent possible, that the rules of all interoperable systems concerned are coordinated in this regard. Unless expressly provided for by the rules of all the systems that are party to the interoperable systems, one system’s rules on the moment of entry shall not be affected by any rules of the other systems with which it is interoperable.”

None of the National Payment System Acts or Bills in force or being considered by SADC Member States contain any reference to, or provisions covering interoperable systems. The Mauritian legal and regulatory framework (in general) nor the specific rules and T&C’s applicable to the ACH and RTGS systems also do not contain any reference to, or provisions covering interoperable systems.

Substantive Content **The Moment of Opening of Insolvency Proceedings**

²⁶ Act 5 of 2003.

²⁷ Act 1 of 2007.

of Law

[Provisions
Concerning
Insolvency](#)

Article 6(1) of the Settlement Finality Directive (As Amended) provides that, “for the purpose of this Directive, the moment of opening of insolvency proceedings shall be the moment when the relevant judicial or administrative authority handed down its decision.”

Most SADC countries do not define the “moment of opening of insolvency proceedings” in their National Payment System Act. Other than Malawi, the only country to do so adequately is Zambia. Section 23(2) of the *Zambian National Payment Systems Act, 2007*²⁸ reads, “Notwithstanding any other law, a winding-up order shall take effect from the minute in the hour and date that it is made against the participant concerned and such order shall not affect any finality of settlement at the end of the settlement cycle.”

Malawi has adopted a detailed and practical solution to determining the moment of opening of insolvency proceedings as set out in the *Payment System Bill, 2014*. This moment is dependent upon the manner in which the insolvency is initiated and the initiating party.

In the case where a participant is wound-up on application by a person other than the Reserve Bank, the winding-up order must record the minute, the hour and the day that such order is made, must be lodged with the Reserve Bank on the same business day and no later than the start of the next business day and served on any other settlement agent to be notified. The Reserve Bank is required to immediately notify all relevant domestic and foreign system operators of the winding-up proceedings.²⁹ This approach is comparable to the approach set out in Article 6(1) of the Settlement Finality Directive (As Amended).”

In the situation where a system participant is wound-up, on application by the Registrar under the *Banking Act, 2009*, or the *Financial Services Act, 2010*, the winding up must state the minute, the hour and the date on which the order is made and the Reserve Bank is required, on the same business day and in any case, no later than the start of the next business day to:

- (a) serve the order on the settlement system participant concerned;
- (b) notify other settlement system participants or agents required to be notified; and
- (c) notify all relevant domestic or foreign system operators.³⁰

Section 24 of the *Malawian Payment System Bill, 2014* covers the situation where a participant is voluntarily wound up. In this case, subject to the provisions of the *Banking Act, 2009*, the *Financial Services Act, 2010* or the *Companies Act, 2013* the system participant that is voluntarily wound up is required to inform all other system participants of the winding-up resolution within twenty four (24) hours of the winding

²⁸ Act 1 of 2007.

²⁹ Section 22 National Payment Systems Bill, 2014.

³⁰ Section 23.

up resolution taking effect. It is important to note that section 24 makes it clear that the resolution, demand or other step to wind-up a settlement system participant or operator has no effect unless approved by the Reserve Bank. As per section 24(2), the Reserve Bank is required to notify relevant domestic and foreign system operators about the voluntary winding up of a settlement system participant on the same day and in any case, no later than the start of the next business day of the winding up resolution taking effect.

The approach taken by Malawi is detailed and thorough and should be considered by other SADC Member States so as to ensure certainty and consistency in this regard.

Despite derogating from Article 6(1) of the Settlement Finality Directive (As Amended) which is simple and concise, the Malawian approach is recommended as it takes cognoscente of the differences in procedure, depending upon the nature of the party instituting the insolvency proceedings.

Notification of the Decision to the Central Bank

Article 6(2) of the Settlement Finality Directive (As Amended) requires that, when a decision has been taken in accordance with paragraph 6(1), the relevant judicial or administrative authority shall immediately notify that decision to the appropriate authority chosen by its Member State.”

The Angolan and Mozambican Laws do not contain a provision such as this and most other Acts have deficiencies with respect to the manner in which the provisions are drafted. Section 12 of Botswana’s National Clearance and Settlement Systems Act, 2003³¹ for example, requires that, “where a participant in a recognised system is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act, the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued shall lodge a copy of the order with the Central Bank.” While they may look similar, section 12 of Botswana’s National Clearance and Settlement Systems Act, 2003 is substantially different to Article 6(2) of the Settlement Finality Directive. In the case of the Settlement Finality Directive, the relevant judicial or administrative authority is required to notify the appropriate authority (the Central Bank) whereas in the case of Botswana’s National Clearance and Settlement Systems Act, 2003 is it “the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued”. It is recommended that the person responsible for notifying the Central Bank of the decision to commence insolvency proceedings should be the relevant judicial or administrative authority that handed down the decision to do so and not, as is the case in Botswana, the person at whose insistence the winding-up or placing under receivership is being carried out.

In terms of section 18(1) of Lesotho’s National Payment System Bill, 2013 a copy of an application for insolvency must be served on the Governor by the Applicant. This

³¹ Act 5 of 2003.

provision should be reworded as it should be a copy of the decision or notification of such decision made by the relevant judicial or administrative authority that is delivered (not served) to the Central Bank of Lesotho. Such notification of the decision to open insolvency proceedings should be made by the relevant judicial or administrative authority and not by the “applicant” as is the requirement in Lesotho’s Bill. In terms of section 18(2), the Central Bank of Lesotho is required to ensure that a copy of the insolvency process is served as soon as reasonably possible to the domestic systems and operators, and if required under international cooperation arrangements with competent foreign authorities to foreign systems or operators. One again, the choice of the word “served” is inappropriate as this has an entirely different implication to simply being notified of a decision to commence insolvency proceedings.

This requirement as set out in sections 22 of the Malawian Payment Systems Bill, 2014 requires that a copy of the winding-up [order] when it is made must be lodged with the Reserve Bank. Section 22 does not however state whether it is the responsibility of the applicant or the relevant judicial or administrative authority to deliver a copy of the order to the Central Bank. It is recommended that this point be clarified.

In terms of section 8(4) of the South African National Payment System Act, 1998 (As Amended),³² “when an application for the winding-up of a clearing system participant or Reserve Bank settlement system participant is made, a copy of (a) the application for winding-up, when it is presented to the court; and (b) any subsequent winding-up order, when it is granted, must be lodged with the Reserve Bank as soon as practicable.” This provision is unclear as to whose responsibility it is to lodge the copy of the winding-up order with the Reserve Bank and should be clarified.

[Notification of the Decision to Other Member States](#)

Article 6(3) of the Settlement Finality Directive (As Amended) introduces the obligations of EU Member States with respect to their obligations to inform other Member States of an insolvency decision and also to inform the European Systemic Risk Board and the European Supervisory Authority (European Securities and Markets Authority). Article 6(3) reads, “The Member State referred to in paragraph 2 shall immediately notify the European Systemic Risk Board, other Member States and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter ‘ESMA’), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council.” Most of the National Payment System Acts that are in force in SADC Member States are applicable to the domestic National Payment System only and do not contain a provision such as Article 6(3).

The DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 is however requires the Central Bank to immediately inform domestic system operators as well as foreign systems and their operators where cooperation agreements provide for this of the opening of insolvency proceedings. It is recommended however that the *Banque Centrale du Congo* should inform other

³² Act 78 of 1998 (As Amended).

Central Banks (regulators) of the commencement of insolvency proceedings, rather than “foreign systems and their operators.” Lesotho’s National Payment Systems Bill, 2013 requires the Governor, upon receipt of notification of insolvency proceedings initiated against a foreign system, operator or participant from a foreign competent authority under an international cooperation arrangement to, as soon as is reasonably possible, notify domestic systems, operators and participants of the initiation of insolvency proceedings.

In the light of the introduction of SIRESS, it is recommended that SADC Member States consider what the appropriate mechanism will be for informing other Member States of an insolvency decision and that such a mechanism is harmonised. It will also be important to consider to which “supranational” structure such a decision must be communicated.

No Retroactive Effects

Article 7 of the Settlement Finality Directive (As Amended) requires that, “insolvency proceedings shall not have retroactive effects on the rights and obligations of a participant arising from, or in connection with, its participation in a system before the moment of opening of such proceedings as defined in Article 6(1). This shall apply, inter alia, as regards the rights and obligations of a participant in an interoperable system, or of a system operator of an interoperable system which is not a participant.”

This requirement is inferred in Article 20 of the Angolan Law nº 05/05 Dated July 29 but is generally considered to be insufficient. While the provision found in Botswana’s Act has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgement of a copy of the order with the Bank. As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgement of a copy of the order with the Bank.

The DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 is one of the few Acts that actually uses the words “retroactive effects.” In this regard, Article 6 reads, “the insolvency proceedings opened for a participant has no retroactive effect on the rights and obligations of a participant from his participation in a system, or in relation with the said participation, before the opening of his insolvency proceedings.”

Section 25 of the Malawian Payment Systems Bill, 2014 has the effect of insolvency proceedings not having retroactive effects. It is however recommended that Malawi consider referring to the “rights and obligations of a participant in an interoperable system, or of a system operator of an interoperable system which is not a participant.”

No provision such as Article 7 of the Settlement Finality Directive (As Amended) is found in the Mauritian law or regulation.

This requirement is inferred in Article 16 of Mozambican Law 02/08 of 27 February but is generally considered to be insufficient.

Section 4(5)(b) of the Namibian Payment System Management Act, 2003 (As Amended)³³ reads, “despite sections 341(2) and 348 of the Companies Act, the winding-up order does not affect any settlement that has become final and irrevocable prior to the lodgement of the copy of that order with the Bank in terms of paragraph (a).” While the Namibian provision has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic.

The provisions found in the Seychelles National Clearance and Settlement Systems Act, 2010³⁴ have the effect of insolvency proceedings not having retroactive effects, however, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. The Act allows for seven days after the commencement of winding-up of a participant). As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgment of a copy of the order with the Bank.

While the South African National Payment System Act does not specifically refer to “insolvency proceedings not having retroactive effects”, this is inferred.

Section 13 of Swaziland’s National Clearing and Settlement Systems Act, 2011³⁵ states, “notwithstanding anything to the contrary in the Insolvency Act, 1955 or the Companies Act, 2009, the winding up of a participant in a recognised or Central Bank system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section 10 before the copy of the relevant order was lodged with the Central Bank in terms of section 12.” While the Swaziland provision has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic.

This requirement is covered by section 20(2) of the Zambian National Payment Systems Act, 2007,³⁶ although the words “retroactive effects” are not used. In terms of section 14 of Zimbabwe’s National Payment Systems Act [Chapter 24:23] “notwithstanding anything to the contrary in the Insolvency Act [Chapter 6:04] or the Companies Act [Chapter 24:03], the winding up of a participant in a recognised payment system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section eleven

³³ Act 18 of 2003 (As Amended).

³⁴ Act 12 of 2010.

³⁵ Act 17 of 2011.

³⁶ Act 1 of 2007.

before the copy of the relevant order was lodged with the Reserve Bank in terms of section thirteen.”

While the Zimbabwean provision has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic.

Substantive Content of Law

Collateral Security

The reduction of credit and systemic risk requires, in addition to the finality of settlement, the enforceability of collateral. This implies that collateral should be insulated from the effects of the insolvency legislation applicable to an insolvent collateral provider (i.e. the collateral taker should be sure that collateral received cannot be challenged in an insolvency procedure).³⁷

The EU approach to the insulation of collateral security is set out in Article 9 of the Settlement Finality Directive (As Amended). Article 9(1) reads, “the rights of a system operator or of a participant to collateral security provided to them in connection with a system or any interoperable system, and the rights of central banks of the Member States or the European Central Bank to collateral security provided to them, shall not be affected by insolvency proceedings against: (a) the participant (in the system concerned or in an interoperable system); (b) the system operator of an interoperable system which is not a participant; (c) a counterparty to central banks of the Member States or the European Central Bank; or (d) any third party which provided the collateral security. Such collateral security may be realised for the satisfaction of those rights.”

Most of the provisions found in National Payment System Acts and Bills are adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context, however most make no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

All fourteen SADC Member States will need to consider amending their domestic legislation to cater for participation in SIRESS. An example of how Article 9(1) of the Settlement Finality Directive (As Amended) was transposed by Ireland into their domestic regulation is provided below. The Irish Statutory Instrument S.I. No. 539/1998 - European Communities (Finality of Settlement in Payment and Securities Settlement Systems) Regulations, 1998 transposes the mandatory provisions of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems into domestic Irish law. Regulation 7(2) of the Irish Statutory Instrument reads, “where securities (including rights in securities) are provided as collateral security to members or to central banks of the Member States or to the European Central Bank, and their right (or that of any nominee, agent or third party acting on their behalf) with respect to the securities is legally recorded on a register, account or centralised deposit system located in a Member State of the European Union, the determination of the rights of

³⁷ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 147.

such entities as holders of the collateral security in relation to those securities shall be governed by the law of that Member State.”

Substantive Content of Law

Most National Payment System Acts / Bills contain a prohibition against payment intermediation. Section 7 of the Namibian Payment System Management Act, 2003 (As Amended)³⁸ is considered to be a well drafted provision and could serve as a benchmark for the proposed harmonised Model Law.

Prohibition Against Payment Intermediation

Substantive Content of Law

The issue of conflict of law was solved in the EU through the Settlement Finality Directive and the Financial Collateral Directive. Both these supranational legal instruments seek to achieve the desired legal certainty for systems’ cross-border operations. Article 9 of each contains rules minimising conflicts of law. These have made a significant contribution to the free cross-border movement of payments and collateral within the EU. The Directives both adopt the “place of the relevant intermediary approach” (PRIMA).

Conflict of Law

Explaining how this principle works, Kokkola states, “Article 9 of the Settlement Finality Directive specifies that where securities (including rights in securities) are given as collateral to a clearing or settlement system or the central bank of an EU Member State and the right of that system or central bank (or that of any nominee, agent or third party acting on its behalf) in respect of the securities is legally recorded in a register, account or centralised deposit system located in Member State X, the determination of the rights of such entities as holders of collateral security in relation to those securities is governed by the law of Member State X. However, that provision applies only to systems and central banks. Consequently, securities provided under other collateral arrangements in the EU are governed by a similar principle (based on Article 9 of the Financial Collateral Directive) concerning the location of the relevant account.”³⁹

Most National Payment System Acts, Bills of Draft Bills do not contain any conflict of law provisions. In light of each SADC Member States current or future participation in SIRESS, this is highlighted as a gap that needs to be rectified.

A good example of such a provision is however found in Article 11 of the DRC’s Draft Law on the Provisions Applicable to National Payment Systems, 2013. This Article which covers the insolvency of a foreign participant in a payment system governed by the DRC’s Act or the insolvency of a domestic (DRC) participant in a foreign payment system reads, “should an insolvency proceeding open against a foreign participant in a payment system governed by this Act, the rights and obligations inherent to the participation of this foreign participant, are entirely and exclusively governed by the Congolese legislation. Should an insolvency proceeding open against a domestic participant in a foreign payment system, the rights and obligations inherent or linked to the participation of this participant to such a system are entirely and exclusively

³⁸ Act 18 of 2003 (As Amended).

³⁹ Kokkola T 2010 *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 150.

governed and determined by the Act governing that foreign system.”

Substantive Content of Law

Dispute Resolution

Most SADC Member States include a dispute settlement provision in their National Payment System Act or Bill. The notable exceptions are the DRC and Lesotho. In the absence of a National Payment System Act in Mauritius, parties to a dispute (either a dispute between the Central Bank and a Participant in the Mauritius Automated Clearing and Settlement System (MACSS) or between two or more parties) are required to follow the dispute resolution mechanism set out in the Mauritius Automated Clearing and Settlement System T&C's.⁴⁰ In Tanzania, in the absence of a legally enforceable National Payment System Act, participants in the Tanzania Inter-Bank Settlement System (TISS) are required to follow the dispute resolution mechanisms set out in the Tanzania Inter-Bank Settlement System Rules and Regulations. In terms of Rule 94, in the case of any dispute arising between the participants with regard to the construction of the Rules and Regulations or the rights, duties or obligations of the participants, including any dispute in respect of and termination of the Agreement to Participate in TISS, such dispute must be referred to arbitration by the Inter-Bank Settlement System Dispute Resolution Committee as established in section 95.

All ten countries that include a dispute settlement provision in their National Payment System Act mandate conciliation, mediation and arbitration as the alternative dispute resolution mechanism. The application of the national Arbitration Act is specifically mandated by eight SADC Member States.

It is specifically noted that none of the National Payment System Acts contain dispute settlement provisions / out of court complaint and redress procedures applicable to payment service providers and payment service users. This matter is covered in Regulation (EC) No 924/2009 on Cross-Border Payments in the Community, and, in light of the introduction of SIRESS and the possible addition of various retail streams in the future, this should be considered by SADC member States. According to Article 11 of the Regulation (EC) No 924/2009, Member States are required to establish adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and their payment service providers. Member States were required to notify the Commission of their out-of-court complaints and redress bodies by 29 April 2010.

International arbitration, as compared to domestic arbitration is a completely different matter. International arbitration needs to accommodate, as far as possible, the wishes of parties from different cultures, both legal and in the wider sense. This means that they need to be able to freely select the nationality of the tribunal, the place of hearings and the extent of court interference. It is also important that foreign arbitral awards are recognised and enforced. In this regard, the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, also known as the "New York Arbitration Convention" or the "New York Convention," is one of the key instruments in international arbitration. The New York Convention applies to the

⁴⁰ The same process is set out in the PLACH Rules.

recognition and enforcement of foreign arbitral awards and the referral by a court to arbitration. Only 9 SADC Member States are contracting parties to the Convention on the Enforcement of Foreign Arbitral Awards (the New York Convention).

It must be noted that Mauritius is positioning itself as the African arbitration seat of choice. Mauritius passed the International Arbitration Act 37 of 2008, which it amended in 2013. Mauritius is a party to the New York Convention. In addition, the 2013 amendments to the International Arbitration Act provide that international arbitration matters will be heard by judges from a panel of "Designated Judges", i.e. these judges will have expertise in international arbitration. Mauritius launched an international arbitration centre, the LCIA-MIAC Arbitration Centre, in 2011. The choice of Mauritius as a viable seat of arbitration for potential disputes that may arise between SIRESS participants should not be ruled out in the future. Such arbitrations would be conducted under the LCIA-MIAC arbitration rules that are universally applicable and suitable for all types of disputes.

[Electronic Documents, Transactions and Signatures](#)

The [UNCITRAL Model Law on Electronic Commerce](#) is based on three fundamental principles, namely, 1) functional equivalence, 2) technology neutrality and 3) party autonomy. Applying these three principles, the Model Law covers the legal recognition of data messages, writing, signatures, originals, admissibility and evidentiary weight of data messages, retention of data messages, formation and validity of contracts, recognition of parties of data messages, attribution of data messages, acknowledgement of receipt and the time and place of dispatch and receipt of data messages.

Most National Payment System Acts in the region do not contain any provisions on electronic documents, transactions, data messages or signatures. Some countries such as Lesotho and the Seychelles have included provisions on the *prima facie* admissibility of electronic and optical evidence, however, if compared to the provisions found in the DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 it is clear that these provisions should be updated and revised. Articles 62 to 66 of the DRC's Draft Law on the Provisions Applicable to the National Payment System covers 1) payment orders kept in archives in electronic format constitute proof and are legally admissible, 2) writing in electronic format is accepted as proof; 3) documents in electronic format must be kept for a period of 10 years, 4) secure electronic signature linked to an electronic certificate are accepted as and carry the evidentiary weight as handwritten signatures, 5) institutions who would like to set up or operate an electronic certification system must be approved by the Central Bank. Even in the case of the DRC, it is recommended that in the absence of an Electronic Transactions and Communications Act that the DRC consider revising these provisions by using the UNCITRAL Model Law on Electronic Commerce (1996) as a best practice benchmark.

Although Mauritius, South Africa and Zambia's National Payment System Acts do not contain provisions on electronic documents, transactions and signatures they have enacted comprehensive Electronic Transactions and Communications Acts. The Seychelles has also enacted a similar Act. These Acts provide evidentiary proof of authentication of electronic payments using digital signatures or other instruments

for electronic payment authorisation. The laws also provide for the establishment and maintenance of a register of cryptography providers and the accreditation of authentication products and services in support of advanced electronic signatures by a recognised Accreditation Authority.

Electronic Money (E-Money)

The emergence of new electronic technologies has resulted in the introduction of new and innovative payment products and services. Advances in Information and Communications Technology (ICT) will continuously influence the payments environment. It is essential for Central Banks to take note of these developments and ensure that appropriate and fit-for-purpose legal provisions are put in place.

Electronic Money (E-Money) has the potential to fundamentally transform the payments domain. It is advisable for all countries in SADC to introduce legislation that regulates the issuance and usage of E-Money. It is however essential that the E-Money regulatory framework is technology neutral and does not constrain itself to a particular form factor or technology platform. The approach adopted by UNCITRAL in the drafting of the UNCITRAL Model Law on Electronic Commerce is recommended in the regard.

Smart card-based E-Money schemes have been launched and are operating in many countries around the world. Network-based or software-based E-Money schemes have been less rapid in their expansion but are nevertheless significant in the payments regulatory environment.

Mobile phone technology is an ideal technology platform to introduce payment products and services. The phenomenal growth experienced by the mobile phone industry together with the mobile phone networks' desire to introduce additional value added services for their clients, has resulted in the emergence of so-called Mobile Money products and services. Mobile Money should however not be regulated in isolation and should be a subset of the bigger E-Money regulatory framework.

There are only two SADC Member States that have issued a legally binding Directive / Determination on E-Money. The DRC's [Directive No. 24 on the Issuance of Electronic Money and Electronic Money Issuing Institutions](#) closely resembles the European Commission Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions as does Namibia's [Payment System Determination \(PSD - 3\) Determination on Issuing of Electronic Money](#) which was issued in 2012. Both of these are excellent regulatory instruments on a par with the international best practice statutory instrument selected for the comparative exercise profiled in this report. It is strongly recommended that Namibia's (PSD - 3) Determination on Issuing of Electronic Money and Directive No. 24 on the Issuance of Electronic Money and Electronic Money Issuing Institutions be considered as appropriate benchmarks for other SADC Member States.

Payment Services

Most SADC Member States do not have a well-structured legal and regulatory framework for retail payments. Vital issues such as electronic money (E-Money), card payments, agent banking, the authorisation of payment service providers (PSPS), the issuance of payment instruments, contractual provisions and the rights and

obligations of PSPs and users are poorly covered.

The PSD is the first piece of legislation that concretely deals with issues in the realm of PSPs and the users of their products. This Directive is a vital building block in the payments legal and regulatory framework and deals with vital issues that have escaped regulatory attention for years. The PSD covers several of the issues noted in the [BIS/World Bank General Principles for International Remittance Services](#) including, Principle 1) Transparency and Consumer Protection; Principle 3) Legal and Regulatory Environment; and Principle 4) Market Structure and Competition.

Title II of the PSD covers the general rules applicable to payment service providers, the designation of competent authorities, supervision, the conditions for the application of the permitted waiver and two common provisions, namely, access to payment systems and prohibition for persons other than payment service providers to provide payment services.

Title III of the PSD covers the transparency of conditions and information requirements for payment services. It includes inter alia the prohibition against charging for information, the derogation from information requirements permitted for low-value payment instruments and E-Money, prior general information requirements for single payment transactions, information requirements for the payer after receipt of a payment order, information requirements for the payee after the execution of a single payment transaction, information and conditions for framework contracts, the ruminant of framework contracts and common provisions on currency and conversion. This is an area that needs addressing in all fourteen SADC Member States.

Title IV covers rights and obligations in relation to the provision and use of payment services (payment instruments). Important issues covered include the authorisation of payment transactions, consent and withdrawal of consent, obligations of payment service providers in relation to payment instruments, notification of unauthorised or incorrectly executed payment transactions, payer's liability for unauthorised payment transactions, refunds, refusal of payment orders, execution time and value date, cash placed on a payment account, right of recourse, data protection and complaints procedures. This is also an area that needs addressing in all fourteen SADC Member States.

It is also important to note that the PSD applies to payment services provided within the community. The payment services falling within the scope of the PSD are as follows:

- 1) services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
- 2) services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
- 3) execution of payment transactions, including transfers of funds on a payment

account with the user's payment service provider or with another payment service provider:

- execution of direct debits, including one-off direct debits;
 - execution of payment transactions through a payment card or a similar device;;
 - execution of credit transfers, including standing orders;
- 4) execution of payment transactions where the funds are covered by a credit line for a payment service user: execution of direct debits, including one-off direct debits;
- execution of payment transactions through a payment card or a similar device;
 - execution of credit transfers, including standing orders;
- 5) the issuing and/or acquiring of payment instruments;
- 6) money remittance; and
- 7) the execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

The EU PSD is applicable to all of the following payment service providers:

- **credit institutions** within the meaning of Article 4(1)(a) of Directive 2006/48/EC (Article 1(1)(a));
- **electronic money institutions** within the meaning of Article 1(3)(a) of Directive 2000/46/EC (Article 1(1)(b));
- **post office giro institutions** which are entitled under national law to provide payment services (Article 1(1)(c));
- **payment institutions** within the meaning of this Directive (Article 1(1)(d));
- **the European Central Bank and national central banks** when not acting in their capacity as monetary authority or other public authorities (Article 1(1)(e));
- **Member States or their regional or local authorities** when not acting in their capacity as public authorities (Article 1(1)(f)).

None of the 14 SADC Member States included in this study have a standalone piece of legislation or regulation in place that has the scope of application that the PSD has.

On the 1 November 2002, Aviso N° 01/2002 was issued in Angola under the powers set out in Article 3 of the Foreign Exchange Law, Law n° 5/97 of 27 June, and Articles 30 and 58 of the *Banco Nacional de Angola* Act -Law n° 6/97 of 11 July. Aviso N° 01/2002 regulates certain aspects related to the provision of payment services under the Payment System of Angola (SPA). Article 2 defines what is meant by a payment transaction and Article 3 defines a payment services as, "a systematic set of procedures provided by the service provider that enables the completion of a payment."

Article 4 states that the provisions of Aviso N° 01/2002 apply to the following payment services:

- "a) receipt by the service provider, or cash payment instrument from the sender to make a payment to the final beneficiary or his legal representative;
- b) the receipt by the service provider, invoice to be paid and the payment instrument and the delivery of those documents to the beneficiary's bank to make bank said final settlement and conclusion of payment to the final beneficiary stated on the invoice, or his legal representative;
- c) the availability of mechanisms of transmission to banks for electronic payment instructions under the Payments System of Angola."

These payment services may be provided by the following entities (Article 6):

- Banks and credit unions (Article 6(1)(a));
- Financial corporations, in accordance with the regulations of their activity (Article 6(1)(b));
- The Postal Administration, according to the Postal Law (Article 6(1)(c));
- Legal non-financial persons, authorised by the National Bank of Angola in accordance with the provisions of Article 7 of Aviso N° 01/2002 (Article 6(1)(d)).

As per Article 5, only authorised institutions, authorised in accordance with the legal and regulatory rules, may provide payment services.

Article 7(2) of Aviso N° 01/2002 requires non-financial legal persons (firms or corporations) with local majority stake holding (capital) to obtain authorisation from the *Banco Nacional de Angola* for the provision of payment services referred to in paragraph a) of Article 4. Non-financial legal persons (firms or corporations) with local majority stake holding (capital) must have:

- share capital not less than USD 250,000.00 (two hundred fifty thousand U.S. dollars), subscribed and fully paid and deposited in the institution domiciled in the country;
- have the object of their activity as being the provision of payment services;
- make adequate provision for technical and technological infrastructure.

Article 8 sets out the requirements and procedure for applications for authorisation of non-financial legal persons (firms or corporations) with local majority stake holding (capital).

Article 9 sets out safeguarding requirements and requires entities providing payment services referred to in paragraph a) of article 4, except banks and credit unions to maintain the “exclusive transit of funds received for payment to the final beneficiary bank account in the provision of this payment service.”

Article 10 reads, “the *Banco Nacional de Angola* may order the cessation of the provision of payment services by any of the entities referred to in this Notice, when the quality of services not meet the objectives of the Payment System of Angola or verify compliance with rules of its subsystems.”

While the DRC does not have a standalone law covering all of the provisions found in the Payment Services Directive, the DRC has adopted a unique approach and is the only SADC country to combine provisions found in “conventional” National Payment System Acts with several of the consumer protection orientated provisions found in the PSD. The drafters of the DRC’s Draft Law appear however to have been highly selective in terms of which PSD provisions they have incorporated into their draft domestic law. Important provisions such as the definition of payment service providers, payment institutions, capital requirements, own funds, safeguarding requirements, authorisation of payment institutions, information requirements for and single payment transactions have been left out.

Some countries have issued related Directives that cover initial capital requirements for E-Money issuers. It must however be noted that, the scope of these Directives is limited to the subject matter that they cover. The DRC’s Directive No. 24 for example only applies to E-Money issuers. The EU PSD covers the capital requirements for all PSPs (payment institutions). Likewise, Namibia’s (PSD - 3) Determination on Issuing of Electronic Money only covers the initial capital requirements of E-Money issuers and not the full scope as set out in the PSD. The same applies to own funds, safeguarding requirements, authorisation and withdrawal of authorisation.

Angola and Mozambique have issued Avisos that apply specifically to “Banking Payment Cards.” These Avisos contain some of the transparency conditions and information requirements as set out in the PSD, but the scope of these Avisos are strictly limited to bank issued cards and not the full range of payment services falling within the scope of the PSD.⁴¹

Tanzania has also adopted a similar approach. Tanzania does not have a standalone law covering all of the provisions found in the Payment Services Directive. The country has also not passed a Consumer Protection Act. The Bank of Tanzania has however stated that the draft National Payment System Bill contains several

⁴¹ Article 2 of Mozambique’s Aviso nº 1/GBM/2014 of 4 June reads, “this Regulation applies to credit institutions and financial companies authorised to issue bank cards, in accordance with applicable law, as well as to the owners and users of these cards.” Similarly, Angola’s Notice No. 09/2011 of 13 October – Rules of Banking Payment Cards applies only to the activities of issuance, acceptance and use of payment cards.

consumer protection provisions which cannot be assessed in terms of scope and content at this time. Tanzania's Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania covers several of the transparency conditions and information requirements and sets out the rights and obligations of E-Money issuers, acquirers, merchants and customers. The Tanzanian Guidelines however only apply to bank issued, card based E-Money products.

While Malawi does not have a standalone law covering all of the provisions found in the Payment Services Directive, several important provisions are found in the Malawian Consumer Protection Act, 2003,⁴² the Payment Systems Bill, 2014 and the Guidelines for Mobile Payment Systems, 2011. It is important to note however that the Guidelines for Mobile Payment Systems, 2011 applies only to mobile financial payment services. Malawi's Consumer Protection Act, 2003 does not cover the specifics as set out in the PSD. The consumer Protection Act does however contain provisions on standard form contracts (section 26), relief against unfair consumer contracts (section 27), contracts governing financial transactions (section 28), the right of retraction (section 30), implied contractual terms (section 31), cancellation and variation of contracts (section 32), consumer information on standards (section 35), the requirement for the price to be displayed (this also refers to services) (section 36), and measures for consumer redress and mechanisms (Part VIII).

Mauritius does not have a standalone Payment Services Law. Several issues covered in the EU's PSD are however covered in the Bank of Mauritius Guideline on Mobile Banking and Mobile Payment Systems, 2013. It is important to note that the Guideline is limited in scope to Mobile Banking and Mobile Payment Systems and does not cover any of the other payment services as listed in the PSD.

South Africa also does not have a standalone Payment Services Law. Several relevant provisions are however found in the Code of Banking Practice which is a voluntary code code that sets out the minimum standards for service and conduct that consumers can expect from their banks with regard to the services and products the bank offers. The Code only applies to personal and small business customers. This Code contains a number of provisions of general application, and is by its nature, not legally enforceable.

[Anti-Money Laundering](#)⁴³

AML/CFT laws and regulations are a vital component of the legal and regulatory framework for payments. The 2012 Financial Action Task Force (FATF) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations contain several recommendations that have direct applicability to payment systems and the provision of payment services.⁴⁴

⁴² Act 14 of 2003.

⁴³ The sections in this report covering Anti-Money Laundering are extracted directly from Langan S and Smith K 2014, *AML/CFT and Financial Inclusion in the SADC: Investigating the Scope for the Harmonisation of Legislation and Regulation on Anti-Money Laundering and Combating the Financing of Terrorism in various Southern African Development Community (SADC) Countries* (Forthcoming Report Commissioned by FinMark) and is included and referenced in this report for ease of reference.

⁴⁴ Financial Action Task Force 2012 *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The Recommendations*.

These include: Recommendation 10, Customer Due Diligence; Recommendation 11, Record Keeping; Recommendation 12, Politically Exposed Persons; Recommendation 13, Correspondent Banking; Recommendation 14, Money or Value Transfer Services; Recommendation 15, New Technologies; Recommendation 16, Wire Transfers; Recommendation 17, Reliance on Third Parties; Recommendation 18, Internal Controls and Foreign Branches and Subsidiaries; Recommendation 19, Higher-risk Countries; Recommendation 20, Reporting of Suspicious Transactions; Recommendation 21, Tipping-off and Confidentiality and Regulation 26, Regulation and Supervision of Financial Institutions. Countries should ensure that the legal framework, in particular the Anti-Money Laundering and Counter Terrorist Financing Law and the Financial Intelligence Centre Law (should such be in place) are compliant with the FATF Recommendations. AML provisions should, where applicable also be included in other legislation and regulation such as any instruments covering correspondent banking, the use of agents, wire transfers and remittance services.

Level of Compliance with FATF Recommendation 10: CDD for “Standard Customers”

Component A: When CDD is required: CDD measures are required for “standard customers” 1) when establishing business relations, 2) when carrying out occasional transactions above the applicable minimum designated threshold (USD/EUR 15 000), 3) carrying out occasional transactions that are wire transfers in the circumstances covered by Recommendation 16 and its Interpretive Note; 4) where is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or 5) where the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Section 15 of the Zimbabwean Money Laundering and Proceeds of Crime Act 2013⁴⁵ is the most compliant provision and it is recommended that the wording of such be used as a benchmark for other SADC countries. All fourteen countries require financial institutions to conduct CDD when establishing a business relationship and conducting an occasional transaction. However, the provision on occasional transactions in several countries does not contain a threshold, or sets a threshold well below the minimum recommended FATF threshold of USD15, 000. The lowest threshold is only equivalent to USD478.51. The only country that has set the threshold at USD 15,000 is Angola. Perhaps the most serious deficiency identified in several countries is the fact that the AML/CFT Law or Regulations do not contain a provision requiring financial institutions to undertake CDD measures when carrying out wire transfers. While several of these countries meet the requirements of FATF Recommendation 16 (Wire Transfers), the CDD provisions in several Acts make no mention of CDD being specifically required for wire transfers that are above the threshold of USD1, 000. Even fewer include the permitted de minimis threshold for occasional wire transfers, below which only the names of the originator and beneficiary and an account number / unique identifier are required.

Component B: Identification measures and verification sources: Component B of FATF Recommendation 10 requires financial institutions to verify the customer’s identity using reliable independent source documents, data and information. All fourteen countries require the standard information such as full name, date of birth,

⁴⁵ Act 4 of 2013.

identity number and nationality. Most require a residential address that must be verified through a variety of acceptable methods/independent verification sources. In some cases, a person's nationality and identity number are not expressly included in the individual countries list of requirements but for the purposes of this analysis, the assumption has been made that if an identity (ID) book / card is required, then the full name, date of birth, identity number and nationality are required. Several countries actually state that official documents must contain a photograph, whilst others simply list documents (ID, passport) that always contain a photograph. For this reason, the assumption that photo ID is required by all has also been made. Tanzania is the only SADC country that requires both a signature and a finger print.⁴⁶ Only three countries, Angola, South Africa and Tanzania require a tax number should such be available. Although Regulation 3(1)(d) of the South African Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended) requires an accountable institution to obtain from, or in respect of, a natural person who is a citizen of, or resident in, the Republic, that person's income tax registration number, if such a number has been issued to that person, Exemption 6(2) exempts all accountable institutions from doing so.⁴⁷ Four countries, Malawi, Namibia, Seychelles and Tanzania require additional contact information (postal address or email or phone number). It is interesting to note that the nature of income and or source of funds is only required by five countries and profession or occupation by six. The information requested, in particular occupation or source of income, nature and location of business activities, if any; and the source of funds involved in the transaction are recognised in most jurisdictions to seem to be a barrier to access to financial services. This is particularly so with respect to individuals that are not banked, trade informally and may not be in formal employment.

All fourteen countries list an ID Document or ID Card and most a Passport as the primary acceptable identification document. Other forms of identification documents such as driver's licenses, birth certificates and voter's cards are accepted in several jurisdictions. In some jurisdictions, passports are only acceptable forms of identification for non-citizens / foreigners while in others, passports are equally acceptable for both nationals/citizens and foreigners / non-citizens. From a financial inclusion perspective, the acceptance of alternative documents for identification and verification purposes is seen as a vital stepping stone to achieving a financially inclusive policy objective. It is therefore vital to note that law and regulation in only six SADC Member States, namely Malawi, Mozambique, Namibia, Seychelles, South Africa and Tanzania permit "alternative documents".

Component C: The timing and verification of identity: The Law and or Regulations in five SADC countries is fully compliant with what this report distinguishes as

⁴⁶It is interesting to note that the Tanzanian Regulation is the only Regulation in the SADC region that requires reporting entities to acquire a signature and thumb print and to provide comprehensive instructions on how the thumb print is to be obtained.

⁴⁷ See De Koker L and Symington J 2011 *Conservative Compliance Behaviour Drivers of Conservative Compliance Responses in the South African Financial Services Industry* 17 where the authors state that, "the regulations also require institutions to obtain the income tax number (if issued) of a customer, but, simultaneously with the release of this requirement, an exemption [Exemption 6(2)] was issued that exempted institutions from obtaining the tax number."

Component C of FATF Recommendation 10. The law or regulation in six countries, namely Botswana, the DRC, Lesotho, Mozambique, Swaziland and Tanzania does not contain a provision or regulation permitting institutions to complete verification as soon as is reasonably practicable after the establishment of a relationship where ML/TF risks are managed and it is essential not to interrupt the normal course of business. While section 16(4) of the *Zambian Financial Intelligence Centre Act, 2010*⁴⁸ states that the Minister may prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of the business relationship if: (a) the risk of money laundering or financing or terrorism is effectively managed; and (b) a delay in the verification is essential not to interrupt the normal conduct of business, at the time of writing of this report, as far as we are aware, these “circumstances” had not been prescribed by the Minister. Likewise, section 16(1) of *Zimbabwe’s Money Laundering and Proceeds of Crime Act, 2013*⁴⁹ states that the Director may, through a directive, prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of business if the risk of money laundering or financing of terrorism is effectively managed and a delay in the verification process is unavoidable in the interests of not interrupting the normal conduct of business.⁵⁰ At the time of the writing of this report, no such directive had been issued.

Four countries do not explicitly require financial institution that are unable to comply (subject to appropriate modification of the extent of measures on a risk-based approach) not to open an account, commence business relations or perform the transaction and consider submitting a Suspicious Transaction Reporting (STR).

[Applying the RBA to CDD: Simplified Measures and Exemptions](#)

A recent Alliance for Financial Inclusion (AFI) / Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) Report, notes that, “most countries surveyed have adopted AML/CFT laws and are developing policy and regulatory frameworks regarding financial inclusion. The region is grappling with the implementation of the 2012 revised FATF Recommendations and especially the new mandatory risk-based approach (RBA) to AML/CFT. At the date of completion of the surveys, none of the countries had yet completed its risk assessment.”⁵¹ The lack of an appropriate legal and regulatory framework and probably more importantly guidelines issued by the regulator and or FIU in each country is potentially a major weakness in several countries.

The AML Law and or Regulations in ten countries mandate the adoption of a risk-based approach, either directly or through inference. Most jurisdictions in SADC started with a purely rules based approach to AML and have slowly introduced the concept of the risk-based approach (RBA) through regulations, exemptions, guidelines and guidance notes. Two countries, namely Namibia and South Africa have

⁴⁸ Act 46 of 2010.

⁴⁹ Act 4 of 2013.

⁵⁰ Section 16(1)(a) and (b) Act 4 of 2013.

⁵¹ Alliance for Financial Inclusion (AFI) and Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2013 *Public and Private Sector Surveys Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices* 8.

elected not to amend their primary AML Acts through the insertion of sections covering the adoption of a RBA, but have instead issued separately gazetted exemptions to sections of the AML Act. Four countries, namely Botswana, the Democratic Republic of the Congo (DRC), Lesotho and Swaziland make no mention of the requirement to adopt a RBA in legislation or regulation or guidelines.

Several SADC countries however include proven low risk exemptions either directly in their primary AML law or regulations or have issued specific exemptions from provisions of the primary AML Act. Others allow for simplified measures in lower risk scenarios. South Africa is the only country that has issued Exemptions for particular types of products / accounts that impose strict requirements with established transaction limits as established by the regulator.

[Level of Compliance with FATF Recommendation 11: Record Keeping](#)

All fourteen SADC countries have record keeping requirements set out in their national AML/CFT Law and or Regulations. The FATF Recommendation 11 requires that documents should be kept for at least 5 years after the termination of a business relationship or after the date of an occasional transaction. SADC countries require records to be kept for a longer period of time, the longest period being 15 years in the case of Mozambique.⁵²

Research has indicated that several countries laws and or regulations on a national level contain inconsistent time periods for which documents are to be kept, i.e. AML/CFT requirements conflict with the other relevant laws. Most SADC countries expressly permit documents to be kept in an electronic format. The exceptions are however the DRC, Swaziland and Zimbabwe. Malawi is the only country in SADC that explicitly requires financial institutions to keep all records in soft copy and hardcopy. As FATF Recommendation 11 does not specifically require that a photocopy (hard copy) of the identification documents presented for verification purposes be kept, it is unclear why there is a need to store a physical copy which makes compliance with Regulation 17(1) an unnecessary burden on financial institutions.

[Level of Compliance with FATF Recommendation 13: Correspondent Banking](#)

The provisions found in AML/CFT laws and or regulations in Angola, Malawi, Mozambique Seychelles, Tanzania, Zambia and Zimbabwe with respect to correspondent banking are compliant with FATF Recommendation 13. Of concern is the fact that correspondent banking is not covered at all in the legal and regulatory frameworks of Botswana and the DRC. This subject matter is also not covered in any guideline or guidance note. Additionally two SADC countries (Mauritius and South Africa) do not cover correspondent banking in law or regulation but have covered this topic in guidelines or guidance notes. It must be emphasised however that requirements found in guidance notes and guidelines are not requirements based in law, regulation or other enforceable means. Seven countries do not have legally enforceable provisions in law or regulation prohibiting banks from entering into or continuing correspondent banking relationships with shell banks.

[Level of Compliance with FATF](#)

The new FATF Recommendation 15 has only recently introduced the requirement that countries and financial institutions should identify and assess the money laundering

⁵² Article 17 Law n° 14/2013.

**Recommendation
15: New
Technologies**

and terrorist financing risks that may arise in relation to the development of new products, business practices and delivery mechanisms. FATF Recommendation 15 requires countries and financial institutions to identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms and (b) the use of new technologies for both new and pre-existing products. The recommendation also requires financial institutions to undertake risk assessments before the launch of new products, business practices or the use of new or developing technologies. Whilst FATF has not released an Interpretive Note for Recommendation 15, it has released a guidance paper on prepaid cards, mobile payments and Internet-based payment services.⁵³ The paper refers to these innovative payment products and services as “new payment products and services” (NPPS).⁵⁴ The paper proposes guidance on the risk-based approach to AML/CFT measures and regulation in relation to NPPS of prepaid cards, mobile payments and Internet-based payment services, in line with the FATF Recommendations. The paper lists several risk factors associated with NPPS that include non-face-to-face relationships and anonymity, geographic reach, methods of funding, access to cash and the segmentation of services. It is important to note that Interpretive Note 10 also lists non-face-to-face business relationships or transactions as a potentially higher risk factor under the category product, service, transaction or delivery channel risk factors.

Despite Recommendation 15 being a new requirement, the AML/CFT Law and or Regulations in six SADC countries, namely Angola, Malawi, Namibia, Tanzania, Zambia and Zimbabwe contain provisions that require financial institutions to develop programmes that include policies and procedures to prevent the misuse of technological developments. The Law and or Regulation in seven countries require financial institutions to apply enhanced CDD measures for non-face-to-face account opening or transactions.

While it can be argued that the requirement to “undertake a risk assessment prior to the launch of a new product, new business practice or the use of new or developing technologies” can conceivably be read into the requirement for financial institutions policies and procedures to prevent the misuse of technological development, none of the fourteen SADC countries expressly require accountable institutions to undertake a risk assessment prior to the launch of a new product, new business practice or the use of new or developing technologies.

**Level of Compliance
with FATF
Recommendation**

Most SADC Member States include a provision on wire transfers (or electronic funds transfer) in their AML law or regulations. The notable exceptions are Botswana, the DRC, Mauritius and Tanzania. The level of compliance of provisions on wire transfers

⁵³ See Financial Action Task Force (FATF) 2013 *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services 4* where the following is stated, “For the purposes of this guidance, NPPS are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations.”

⁵⁴

16: Wire Transfers

in law and regulation varies across countries.

The scope, ambit and implications of the de minimis threshold as reformulated in FATF Recommendation 16 is succinctly summarised by the European Commission DG Internal Market and Services (DG MARKT) as follows:

“The de-minimis threshold of USD/EUR 1,000 has been retained in the new Recommendation; however, the new Recommendation spells out clearly what information is still required for international wire transfers under this threshold. This includes the names of the originator and the beneficiary as well as the account number of both parties. The latter can be replaced by a unique transaction reference number. The address/national ID number/customer ID number/date and place of birth are no longer required. The accuracy of the information need only be verified in the case of suspicion of money laundering.”⁵⁵

The manner in which the de minimis threshold has been included in two AML Laws passed by SADC Member States post the release of the revised FATF Recommendations provides insight into how countries have chosen to interpret the flexibility provided by Recommendation 16. The Zimbabwean interpretation of Recommendation 16 is interesting in that section 27 of the Money Laundering and Proceeds of Crime Act, 2013⁵⁶ includes the de minimis threshold of USD1,000 but the manner in which section 27 is drafted seems to imply that all wire transfers, be they domestic or cross-border transfers, occasional or regular, that are below the USD1,000 threshold are exempt from the requirements set out in sections 27(1)(a) – (d). This is not the intention behind the exemption for occasional cross-border wire transfers as set out in the Interpretive Note to Recommendation 16.

A similar problem is evident in the drafting of Article 15 of Mozambique’s Law n° 14/2013. While the thirty thousand meticaïs set in Article 15(4)(c) is equivalent to USD 946.53 and within the USD 1,000 de minimis threshold permitted by FATF Interpretive Note 16, paragraph 5 it is contradictory to the threshold listed in Article 10(1)(b) of Law n° 14/2013 which applies to both domestic and international transfers. Article 15(4)(c) of Law n° 14/2013 also appears to be in contravention of FATF Interpretive Note 16, paragraph 5 as the Mozambican provision states quite clearly that the provisions set out in Articles 15(1) to 15(3) are not applicable to transactions within the maximum limit of thirty thousand meticaïs. This means that financial institutions do not have to ensure that they obtain originator and beneficiary information or that such information must accompany the transfer or that the information must accompany the relevant message over the course of the chain of payments, or that where an originator does not have a bank account, that one reference number must be attributed to the transaction.⁵⁷ It therefore appears that the drafters of the new law have misunderstood the flexibility permitted by the Interpretive Note to FATF Recommendation 16 which allows countries to permit financial institutions not to have to **verify** the name of the originator, the name of the beneficiary and the account

⁵⁵ European Commission DG Internal Market and Services (DG MARKT) 2013 *Additional Research to Assess the Impact of Potentially Changing the Scope (Art. 3) of the Regulation on Information Accompanying Transfers of Funds* 14.

⁵⁶ Act 4 of 2013.

⁵⁷ See Article 15(2) Law n° 14/2013.

number for each or a unique transaction number for occasional cross-border wire transfers below the threshold of USD1, 000. This information should however still be provided.

[Level of Compliance with FATF Recommendation 17: Reliance on Third Parties](#)

Most SADC Member States AML/CFT Laws and or Regulations contain provisions permitting financial institutions to rely on third parties to perform several CDD measures and introduce business. Notable exceptions are Botswana, DRC, South Africa and Tanzania. In Botswana, section 13 of the Financial Intelligence Agency Act, 2009⁵⁸ allows for record keeping obligations set out in section 11 of the Act to be performed by a third party but the Financial Intelligence Agency Act, 2009 is silent on CDD obligations being undertaken by third parties. The DRC Law 04/016 does not contain any provisions related to reliance on third parties. In South Africa, the only reference made to reliance on third parties in the Financial Intelligence Centre Act, 2001 (As Amended)⁵⁹ is with respect to an accountable institution's record keeping obligations (section 22). The Financial Intelligence Centre Act, 2001 (As Amended) does not contain any provisions permitting accountable institutions to outsource CDD requirements to third parties. PCC12 Outsourcing of Compliance Activities to Third Parties which was issued by FIC in 2012 however clear states, "An accountable institution may utilise the services of a third party to perform activities relating to the establishing and verifying of clients' identities as well as the collection of required documents to establish and verify the identity of their clients, and for record-keeping purposes as required in terms of the FIC Act and the Regulations to the FIC Act. However, an accountable institution remains liable for compliance failures associated with and/or caused by such an outsourcing arrangement."⁶⁰

[Level of Compliance with FATF Recommendation 20:STRs](#)

All fourteen SADC countries AML/CFT Law and or Regulations contain a provision on suspicious transaction reporting and in all cases; suspicious transactions including attempted transactions must be reported to the financial intelligence unit. A lack of coordination, conflicting legislation and conflicting messages with respect to the reporting of suspicious transactions has however been highlighted by a number of countries as an area of concern. Given the infancy of the RBA and the fact that very few SADC Member States have embraced this concept, many do not yet provide guidance on the application of the RBA for the purpose of **identifying** potentially suspicious activity, for example, by directing resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk. It must be noted however, the RBA does not extend to the **reporting** of STRs

⁵⁸ Act 6 of 2009.

⁵⁹ Act 38 of 2001 (As Amended).

⁶⁰ In terms of Exemption 5 to the Financial Intelligence Centre Act, 2001 (As Amended), every accountable institution is exempted from compliance with the provisions of Section 21 of the Act which require the verification of the identity of a client of that institution if: a) that client is situated in a country where, to the satisfaction of the relevant supervisory body, anti-money laundering regulation and supervision of compliance with anti-money laundering regulation, which is equivalent to that which applies to the accountable institution is in force, b) a person or institution in that country, which is subject to the antimoney laundering regulation referred to in paragraph (a) confirms in writing to the satisfaction of the accountable institution that the person or institution has verified the particulars concerning that client which the accountable institution has obtained in accordance with Section 21 of the Act, and c) the person or institution referred to in paragraph (b) undertake to forward all documents obtained in the course of verifying such particulars to the accountable institution.

[Compliance with FATF Recommendation 34: Guidance and Feedback](#)

according to the new standard – all STRs must be reported to the FIU.

The Financial Intelligence Units in all fourteen SADC countries are empowered to issue guidelines and guidance notes. The wording of these sections in either the AML Law or its supporting regulations differs from country. Some drafters have used the words “may issue guidelines”, which upon the normal interpretation of these words infers that the issuing of guidelines is at the discretion of the FIU while others have used the words “shall issue guidelines.” Guidelines and or guidance notes have not been issued by the FIU, the Central Bank or other Supervisory Authorities in five SADC countries.

[SADC Wide Findings & Recommendations](#)

This project has revealed substantial differences in the regulatory models adopted, the level of sophistication of the legal and regulatory framework, differences in legal traditions (civil law v common law), available infrastructure - Real Time Gross Settlement System (RTGS), Automated Clearing House (ACH) and National Switches, organisational capacity and the overall approach to the regulation and oversight of the National Payment System, in each country. While countries such as Namibia and South Africa have advanced legal frameworks, others such as the DRC, Lesotho, Malawi, Mauritius and Tanzania do not have a National Payment System Act in place. As such, vital provisions that are applicable to the regulation and oversight of their domestic National Payment System, such as settlement finality and irrevocability, access criteria, transfer orders and netting, the insulation of collateral security from the effects of insolvency law and general override provisions in the case of curatorship, judicial management or liquidation do not exist in a legally enforceable Act.

For countries that do have a legally enforceable National Payment System Act or Payment System Management Act in place, several gaps and inconsistencies across the legal and regulatory frameworks have been identified. When compared against the international best practice hard law benchmark used for the purposes of undertaking a benchmarking exercise, namely the EU Regulations and Directives, it is apparent that none of the National Payment System Acts applicable domestically contain any provisions pertaining to cross-border relations and transactions. In light of the introduction of SIRESS, it is vital that domestic laws are harmonised, that regulators are legally mandated to cooperate with each other and that provisions pertaining to cross-border payment arrangements are included in domestic laws. A particular area of concern is the choice of an appropriate regional dispute resolution mechanism and fora. While several National Payment System Acts contain provisions for the choice of conciliation, mediation and arbitration as the means to resolve disputes between participants in domestically designated systems, none of the Acts contain provisions on international arbitration, the choice of law or appropriate fora. It is also specifically noted that none of the National Payment System Acts contain dispute settlement provisions applicable to payment service providers and payment service users. This matter is covered in Regulation (EC) No 924/2009 on Cross-Border Payments in the Community, and, in light of the introduction of SIRESS and the possible addition of various retail streams in the future, this should be considered by SADC Member States.

Most countries do not have a well-structured legal and regulatory framework for retail

payments. Vital issues such as electronic money (E-Money), card payments, agent banking, the authorisation of payment service providers, the issuance of payment instruments and the rights and obligations of PSPs and users are, in the most part, set out in guidance notes, guidelines and position papers. These by their very nature are not legally enforceable and the Central Bank as the sector regulator generally has no powers, other than moral suasion to enforce them. The lack of law and regulation in the SADC region covering these matters is highlighted as an additional area of concern.

Individual SADC Member States are at liberty to amend their domestic laws and regulations as they see fit, however, we recommend that this is carried out in a coordinated manner through the drafting of a model law(s). Several SADC Protocols including the Protocol of Finance and Investment require State Parties to create Model Laws for the Region. Article 2 of Annex 5 of the Protocol on Finance and Investment requires State Parties to “promote the mutual co-operation, co-ordination and harmonisation of the legal and operational frameworks of Central Banks which shall culminate in the creation of a Model Central Bank Statute for the Region as contemplated by the RISDP.” It must be noted that Model Laws are by their very nature, “soft laws” and are not legally enforceable. They are however generally used to guide governments in the crafting and amendment of their own domestic laws. Model Laws are primarily aimed at assisting member states, in particular policy makers and legislative drafters to address all the relevant areas in need of legislative reform without usurping the authority of national legislatures. In an article entitled *Judges Welcome SADC Model Law on HIV/AIDS* the author notes that, “an important benefit of the Model law is that it builds on the collective experiences of other legislatures, providing a pool of wisdom from which a particular legislature may select and adapt provisions to suit its own circumstances and needs.”⁶¹

Given the current organisational and institutional limitations of the SADC it is submitted that appropriate instruments to be drafted to spearhead the harmonisation process at this time, are model laws that could be used by each SADC Member State as best practice benchmarks.

The recommendations below are high priority short-term action areas.

Recommendation 1: Glossary of Key Terms

Section 2.3.2 of each country report highlights substantial gaps in each country’s defined terms. Where terms are defined, significant differences in the definitions used have also been identified. It is highly recommended that a glossary of key terms is prepared.

Recommendation 2: Model Laws (Payments)

⁶¹ Magadza M 2009 *Judges Welcome SADC Model Law on HIV/AIDS*. Online. Available at: <http://www.africafiles.org/article.asp?ID=22152>

At present, a harmonised legal and regulatory framework for payments does not exist in SADC and the region also faces a number of organisational and institutional challenges. The SADC Central Bank is yet to be established and SADC does not have a Parliament with legislative powers as in other similar institutions such as the EAC, EU and ECOWAS. There are no SADC Regulations and or Directives on Payments (Annex 6 of the Finance and Investment Protocol however establishes a framework for cooperation and coordination between Central Banks on payment, clearing and settlement systems) and the SADC Tribunal remains disbanded. As a result, the SADC Member States participating in the SIRESS proof of concept project have elected to structure the legal arrangements between participants through a number of multilateral agreements. These agreements have been drafted as a short term solution in order to provide for legal certainty until such time as an appropriate SADC wide legal and regulatory framework has been developed and adopted. Over the longer term, all fourteen SADC countries are committed to harmonising their legal and regulatory frameworks and to establishing the institutional and organisational structures conducive to the establishment of an integrated payments market.

As a key starting point in the harmonisation process, it is recommended that two SADC payments related model laws be drafted for consideration. These would be a Payment Systems Law to harmonise the provisions found in the current National Payment System Law in each SADC country and a Payment Services Law to introduce a harmonised legal framework for payment services thereby ensuring that cross-border payments within the SADC (particularly credit transfers, direct debits and card payments) can be carried out just as easily, efficiently and securely as domestic payments within the various Member States. These two Model Laws should be drafted taking into consideration international best practice principles, best practice provision drawn from the domestic law of SADC Member States and making use of the various EU Regulations and Directives as they pertain to specific cross-border matters.

Although Annex 12 to the FIP does not promote the drafting of a SADC Model AML/CFT Law, article 6(1) does state that, "regional coordination will promote efficiency and promote arbitrage between State Parties." It is also recommended that the SADC Anti-Money Laundering Committee consider commissioning the drafting of a Model AML/CFT Law or a Regional Guideline for the SADC.

Recommendation 3: AML Model Law

In theory, Article 9(3) of Annex 12 of the Protocol on Finance and Investment (FIP) establishes the SADC Anti-Money Laundering Committee. In practice however, this Committee has not been constituted and is therefore not, at this point in time, an official SADC structure. It is therefore recommended that the AML specific recommendations contained in this report be considered, in the short term, by an existing SADC structure which has appropriate decision making powers in order to avoid the risk of in-action or substantially delayed action while the SADC Anti-Money Laundering Committee is being constituted. In order to move forward towards the defined level of harmonisation and so as not to be delayed by institutional matters, it is recommended that each SADC country be encouraged and guided by a duly

mandated existing SADC structure, potentially the CCBG Legal-Sub Committee or the SADC Payment Steering Committee as duly mandated by the CCBG, to obtain a defined level of legislation and regulation at a national level in line with the revised FATF Recommendations (2012). It is recommended that the focus of mandated existing SADC structure should be directed towards:

- A: the drafting of an appropriate SADC Model AML/CFT Law and support being provided to domestic regulatory authorities during the process of amending domestic AML/CFT laws and regulations;
- B. the commissioning and undertaking of a supra-national SADC wide risk assessment;
- C: the preparation of a short term action plan and a longer term hand-over plan. It is recommended that the mandated SADC structure work collaboratively with the ESAAMLG so as to avoid the duplication of efforts and resources.

Recommendation 4: Scoping Study and Preparation of an Electronic Money Guideline for SADC

The review of the statutory instruments regulating E-Money in Namibia and the DRC, as compared to the E-Money guidelines issued by various central banks has highlighted significant differences in *inter alia*: the understanding and definition of E-Money; whether E-Money constitutes deposit taking or not; conditions for authorisation; initial capital, own funds and safeguarding requirements. It is recommended that in order to assist Central Banks in the SADC to adopt a consolidated approach to E-Money that an in-depth study on the concept of E-Money in SADC should be undertaken, which should culminate in the drafting of an E-Money guideline for the SADC region.⁶² This work should be undertaken at the same time as the drafting of the Model Laws as these matters are not mutually exclusive and cross references to specific provisions should be made in the Model Laws and the E-Money Guideline.

Country Specific Recommendations

Country specific recommendations are set out in the fourteen country reports (Volume I and II) that form an integral part of this report. These country specific recommendations are framed within the context of the primary overall recommendation for SADC that a Payment System Model Law and Payment Services Model Law are developed. As such, there is convergence in several of the recommendations made. The proposed Model Law will draw upon international best practice together with regional best practice benchmarks as discussed throughout this report.

There are a number of vital issues that need to be addressed by each Central Bank and other relevant regulatory authorities within each domestic context. While each SADC Member State is at liberty to pass new laws and or make changes to existing

⁶² Activities include, determining a common definition and understanding of E-Money, regulatory principles, and policy and drafting a SADC specific regulatory framework in the form of a guideline.

legislation of its own accord, it is strongly recommended that amendments to the National Payment System / Payment System Management Act / Clearing and Settlement System Acts and the Anti-Money Laundering Acts are made in accordance with the provisions contained in the proposed SADC Model Laws.

SECTION 1: INTRODUCTION

At its meeting held in Pretoria in May 2009, the Committee of Central Bank Governors (CCBG) of the Southern African Development Community (SADC), granted approval for the initiation of the SADC Payment System Integration project.⁶³

At the core of this project is the testing of the SADC Integrated Regional Electronic Settlement System (SIRESS) in the four Common Monetary Area (CMA) countries, namely, Lesotho, Namibia, South Africa and Swaziland. As noted by the SADC Payment Clearing and Settlement Subcommittee, “a crucial aspect of the proposed SADC cross-border payment system model is that it is based on a single currency. The CMA environment allows for the integrated solution to be tested and implemented in a ‘single currency’ environment, even while issues around convergence in SADC integration are still being resolved. Should the schedule on the [Regional Indicative Strategic Development Plan] RISDP⁶⁴ be delayed, and the introduction of the SADC currency be re-scheduled for a later date, using the CMA environment, testing and implementation of the SADC cross-border payment system would not be delayed.”⁶⁵

The SIRESS Proof of Concept (POC) in the CMA went live on the 22 July 2013 and the second phase, opening participation to the system to some of the non-CMA SADC countries, commenced in October 2013. During the POC phase of the project, the South African Reserve Bank is hosting and operating SIRESS. All participants in the settlement system are required to have accounts in SIRESS as ordinary members. The South African Reserve Bank, on behalf of the SIRESS participating Central Banks, is therefore the operator of the system and at the same time is also a participant.⁶⁶

The introduction of The Trans-European Automated Real-time Gross Settlement System (TARGET) and later TARGET2⁶⁷ can be seen as the first tangible step towards the Single Euro Payments Area (SEPA) in the European Union.⁶⁸ In a similar vein, the launch of SIRESS will be the first tangible payments infrastructure related step towards an integrated SADC. The key focus of both the TARGET2 and SIRESS systems is to permit

⁶³ Southern African Development Community (SADC) Payment Clearing and Settlement Subcommittee 2011 *SADC Payment System Integration using the Common Monetary Area as Proof of Concept*.

⁶⁴ The Regional Indicative Strategic Development Plan is a comprehensive development and implementation framework guiding the Regional Integration agenda of the SADC over a period of fifteen years (2005-2020). It is designed to provide clear strategic direction with respect to SADC programmes, projects and activities in line with the SADC Common Agenda and strategic priorities, as enshrined in the SADC Treaty of 1992.

⁶⁵ Southern African Development Community (SADC) Payment Clearing and Settlement Subcommittee 2011 *SADC Payment System Integration using the Common Monetary Area as Proof of Concept – 2011-09-05*.

⁶⁶ Central Bank of Lesotho “The Southern African Development Community Integrated Regional Settlement System (SIRESS): What? How? Why?” 2013 *CBL Economic Review* (145) 1.

⁶⁷ The European System of Central Banks (ESCB) is composed of the European Central Bank (ECB) and the national central banks (NCBs) of all 28 European Union (EU) Member States.

⁶⁸ The Trans-European Automated Real-time Gross Settlement System (TARGET2) was launched by the Eurosystem (the ECB and national EU central banks) in November 2007. TARGET2 is based on a Single Shared Platform (SSP) providing a harmonised service level at a uniform price over a standard interface with access via the SWIFT network (Y-copy) using SWIFT messages.

banks across the EU and SADC respectively to benefit from real-time payment processing with intraday settlement finality.⁶⁹

The SADC Payment System Integration project is divided into four different payment work streams. The launch and testing of SIRESS is the first of these streams.⁷⁰ At the same time, the SADC Bankers Association (SADCBA) is currently working on:

- a) A regional clearing capability for Electronic Funds Transfer (EFT) credits and debits;
- b) A regional clearing capability for Card and ATM transactions;
- c) Initiating a work programme with the Committee of SADC Stock Exchanges (COSSE) to explore regional Central Securities Depositories.

The SADC Payment System Integration project, to a large extent, seeks to replicate the achievements in Europe. As stated publically by Tim Masela of the South African Reserve Bank, "this project is patterned explicitly after the SEPA."⁷¹ Williams, quoting Tim Masela states, "There is a common currency target for the region of 2018 and we want to make sure that any new infrastructure can support it. The experience in Europe is very useful".⁷²

Key to the establishment of an integrated payments market in the EU was the development of a single market which has been under construction in the European Union since 1973. The changeover to the Euro in 1999 resulted in the creation of a single money market in Member States that adopted a single currency. However, as noted by the European Central Bank, "in order to develop and ensure the provision of efficient payment and securities services, fair competition and an appropriate level of protection for the users of such services, it is essential to remove not only technical, but **legal barriers**. Only a modern and efficient legal framework is capable of guaranteeing the safety, soundness and efficiency of payments, securities transactions and financial collateral arrangements, ensuring that legal certainty exists for all parties involved in the process."⁷³

Since 1998 a number of binding legal instruments pertaining to payments, have been adopted in the EU. These include both regulations and directives. Regulations are the most direct form of European Union (EU) law. As soon as they are passed, they have binding legal force throughout every Member State, on a par with national laws. National governments do not have to take action themselves to implement EU regulations. They are different from directives, which are addressed to national authorities, who must then take action to make them part of national law, and decisions, which apply in specific cases only, involving particular authorities or individuals. Regulations are passed either jointly by the EU Council and European Parliament, or by the Commission alone.⁷⁴ Three regulations pertaining directly to payment systems have been passed since 2001. These cover cross-border payments in Euro, information on the payer accompanying transfers of funds and

⁶⁹ See Wandhöfer R *EU Payments Integration: The Tale of SEPA, PSD and Other Milestones Along the Road* (2010) 45 where the author notes that, "the system permitted banks across the EU to benefit from real-time payment processing with intraday settlement finality and most importantly facilitated the rapid integration of the EU money market and associated business practices (until then rather fragmented). The key focus of the TARGET system was to enable high value inter-bank operations and thus in itself became instrumental in reducing systemic risk."

⁷⁰ The "Credit Transfers Requiring Immediate Settlement" stream was implemented in July 2013.

⁷¹ Juri G "Out of Africa" 2011 *CLEARIT: The Swiss Professional Journal of Payment Traffic* 47 15.

⁷² Williams M *Pilot Plan to Harmonise Payment Infrastructure in Southern Africa*.

⁷³ Kokkola T *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* (2010) 231.

⁷⁴ See http://ec.europa.eu/eu_law/introduction/what_regulation_en.htm

technical and business requirements for credit transfers and direct debits in Euro. Regulation 2560/2001 which was later repealed by Regulation 924/2009 is widely recognised as the foundation of SEPA.⁷⁵

EU directives on the other hand, require certain end results that must be achieved in every Member State. National authorities have to adapt their laws to meet these goals, but are free to decide how to do so. Directives may concern one or more Member States, or all of them. Each directive specifies the date by which the national laws must be adapted, giving national authorities the room for maneuver within the deadlines necessary to take account of differing national situations. Directives are used to bring different national laws into line with each other, and are particularly common in matters affecting the operation of the single market. Over time, the EU legislature's focus has broadened to cover various, increasingly complex aspects of payment and securities systems with the adoption of the following directives: the Settlement Finality in Payment and Securities Settlement Systems (Directive 98/26/EC) as amended by Directive 2009/44/EC; the Community Framework for Electronic Signatures (Directive 1999/93/EC); the Taking-up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions (Directive 2009/110/EC) which repealed Directive 2000/46/EC; Directive 2002/47/EC on financial collateral arrangements as amended by Directive 2009/44/EC; Directive 2004/39/EC on markets in financial instruments (MiFID), which replaced Directive 93/22/EC on investment services in the specified securities field.⁷⁶

At present, a harmonised legal and regulatory framework for payments does not exist in SADC and the region also faces a number of institutional challenges. The SADC Central Bank is yet to be established and SADC does not have a Parliament with legislative powers as in other similar regions such as the EAC, EU and ECOWAS. There are no SADC Regulations and or Directives on Payments (Annex 6 of the Finance and Investment Protocol however establishes a framework for cooperation and coordination between Central Banks on payment, clearing and settlement systems)⁷⁷ and the SADC Tribunal remains disbanded. As a result, the SADC Member States participating in the SIRESS proof of concept project have elected to structure the legal arrangements between participants through a number of multilateral agreements.⁷⁸ These agreements have been drafted as a short term solution in order to provide for legal certainty until such time as an appropriate SADC wide legal and regulatory framework has been developed and adopted. Over the longer term, all fourteen SADC countries are committed to harmonising their legal and regulatory frameworks and to establishing the institutional and organisational structures conducive to the establishment of an integrated payments market.

This *Legal and Regulatory Framework for Payments in 14 SADC Member States (2014)* and 14 Country Reports (Volume I and Volume II) were commissioned by FinMark Trust with the support of the SADC Payment System Subcommittee and Committee of Central Bank Governors (CCBG) Legal Subcommittee as the first step in a long journey towards a harmonised legal and regulatory framework for payments in the SADC.

⁷⁵ European Payments Council 2009 *Making SEPA a Reality: The Definitive Guide to the Single Euro Payments Area*.

⁷⁶ See Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 232 where it is noted that, "to some extent, specific provisions on solvency ratios in Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions (the "Banking Directive") and Directive 2006/49/EC on the capital adequacy of investment firms and credit institutions (the "Capital Adequacy Directive") are also relevant."

⁷⁷ The SADC Summit has power to legislate pursuant to Article 10.3 of the SADC Treaty which clearly states that 'the Summit shall adopt legal instruments for the implementation of the provisions of this Treaty; provided that the Summit may delegate this authority to the Council or any other institution of SADC as the Summit may deem appropriate'.

⁷⁸ There are currently three agreements and an MOU in place. These are the SIRESS Stakeholders Agreement, SIRESS Settlement Agreement, SIRESS Service Agreement and Schedules and the MOU for SADC Payment System Oversight.

This Master Report together with the fourteen detailed country reports provide an overview of the legal and regulatory framework for payments in each SADC Member State. The Master Report and 14 country reports compares the provisions found in domestic law and regulation of each SADC Member State with similar provisions found in law and regulation applicable in other SADC Member States through a process of peer review, and identifies relevant gaps in the current legal and regulatory framework. As far as possible, the substantive content of laws, regulations, determinations, directives and guidelines that are in force and have been issued in by each SADC Member State are measured against several international best practice principles (soft laws) including the Principles for Financial Market Infrastructures (PFMIs) and the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations (2012).

In addition, as the SIRESS project is modelled on SEPA, the regulatory framework adopted by the EU serves as an appropriate benchmark when considering the harmonisation of payment, clearing and settlement system laws and regulations in the SADC region. The provisions included in the three primary EU Regulations adopted together with best practice principles drawn from several EU Directives are used as a benchmark for the assessment of the substantive provisions found in laws and regulations.

This Master Report is divided into 12 sections as follows:

- Section 1:** Introduction
- Section 2:** Harmonisation of Payment System Laws in SADC
- Section 3:** International Best Practice: The Choice of Soft Law and Hard Law Benchmarks
- Section 4:** Domestic Legal and Regulatory Frameworks in SADC
- Section 5:** Review of each SADC Member States Primary Payments Statute
- Section 6:** Electronic Documents, Transactions and Signatures
- Section 7:** Electronic Money
- Section 8:** Payment Services
- Section 9:** Anti-Money Laundering
- Section 10:** Recommendations

SECTION 2: HARMONISATION OF PAYMENT SYSTEM LAWS IN SADC

The harmonisation of payment system law in SADC, will in the most part, be dependent upon individual SADC Member States being willing to amend their domestic law in line with the Payment System Model Law and Payment Services Model Law proposed.

While the legal basis for the harmonisation of Payment System Law in the SADC region is found in the Annex 6 of the Protocol on Finance and Investment (FIP), unlike Article 2 of Annex 5 of the FIP that requires State Parties to “promote the mutual co-operation, co-ordination and harmonisation of the legal and operational frameworks of Central Banks which shall culminate in the creation of a Model Central Bank Statute for the Region as contemplated by the RISDP”⁷⁹ article 6(1)(c) of Annex 6 does not require the creation of a Payment System Law. Instead, the article states simply that, “the SADC Payment System Steering Committee shall consider and recommend the enactment of, or amendments to, legislation of State Parties relating to payment systems, clearing systems and settlement systems, including the making and amendment of rules and procedures, risk management policies and any other matters relevant to such legislation and such payment systems, clearing systems and settlement systems.”

Given the current institutional structure of SADC, the lack of consensus on whether the Summit or the Council has the power to, (as is the case in the EU), to promulgate binding regulations that would have force of law in each SADC Member State without the need for any act of acceptance or incorporation into the domestic, it appears that the only option at this time is to propose the drafting of a Payment System Model Law. Such a Model Law must have the status of soft law to inform policy making in each SADC Member State. As such, it must be developed under the auspices of one of the SADC structures fully mandated to do so by the SADC Treaty (see section 2.1 below).

As noted by Faria, there are often general problems associated with international and or regional rule making. In this regard, Faria states,

“The search for consensus between different legal traditions is not an easy enterprise level, and international [or regional] uniform rules are often subject to criticism by domestic readers, who point out the superiority of national law over the product of international [or regional] negotiation – if not in substance, at least in style. As any other product of human labour international [or regional] conventions are often imperfect and indeed the circumstances under which the harmonisation process take place are not ideal. At the domestic level, legislation is drafted in the national language system, in the context of the domestic legal system and by persons who are knowledgeable about it. It usually provides an opportunity for taking into account and solving possible problems for coordination or conflict of pre-existing law. That is not the case when a legal text is prepared at the international [or regional] level for introduction into domestic systems. [...] The legal text is to a large extent drafted in the abstract, i.e. in a generic form that may have to be adapted to local circumstances. If it is done well, it will be drafted in clear language, will not use words with particular meanings in specific legal systems and will be easy to translate with a low likelihood of error. The result will almost assuredly be a style of drafting unfamiliar to many versed in the national legislation of their own country.”⁸⁰

⁷⁹ Article 3(d) of Annex 5 reads, “the objectives of this Annex are to: provide the framework for the creation of a Model Central Bank Statute which shall be considered and approved by the Ministers responsible for national financial matters.”

⁸⁰ Faria J “Legal Harmonisation Through Model Laws: The Experience of the United Nations Commission on International Trade Law (UNCITRAL)” 2005 8.

As an introduction to the remainder of the report, the sections below briefly discuss the SADC institutions and structures, the legal status of SADC instruments (the SADC Treaty, Protocols, Model Laws, MOU's and TA's) and the legal basis for harmonisation.

2.1 The SADC Institutions and Structures

Founded in 1992, SADC was the successor organisation to the Southern African Development Coordination Conference (SADCC) that was established in 1980.⁸¹ When SADC was formed, the Treaty⁸² provided for several main organs. These were the Summit, the Committee of Ministers, the Secretariat and the Standing Committee of Officials. Later, in August 2002, Article 9(1) of the Treaty was amended to provide for *inter alia*: the Organ on Politics, Defence and Security Cooperation (OPDSC) and the Tribunal.⁸³ In SADC, the only institutions whose decisions are described as expressly binding in the Treaty are the Summit and the Tribunal.

Diagram 1: SADC Institutional Framework



2.1.1 The Summit

The Summit consists of the Heads of State or Government of all Member States and is the supreme policy making Institution of SADC. In terms of Article 10(3) of the SADC Treaty, it is the Summit that is empowered to

⁸¹ Musavenga T 2011 *The Proposed SADC Parliament: Old Wine in New Bottles or an Ideal Whose Time Has Come?* 11.

⁸² Treaty of the Southern African Development Community

⁸³ The Tribunal was suspended at the 2010 SADC Summit. It is however noted on the SADC website that, "On 17 August 2012 in Maputo, Mozambique, the SADC Summit addressed the issue of the suspended SADC Tribunal. The SADC Summit resolved that a new Tribunal should be negotiated and that its mandate should be confined to interpretation of the SADC Treaty and Protocols relating to disputes between Member States."

“adopt legal instruments for the implementation of the Provisions of the Treaty.” The Summit may however delegate this authority to the Council or any other SADC institution.

In Doctoral Thesis, *The SADC Tribunal and the Judicial Settlement of International Disputes*, Zenda puts forward the opinion that, “the SADC Summit has the power to legislate pursuant to Article 10(3) of the Treaty which clearly states that ‘the Summit shall adopt legal instruments for the implementation of the provisions of this Treaty; provided that the Summit may delegate this authority to the Council or any other institution of SADC as the Summit may deem appropriate. There is no good reason to suppose that legal instruments adopted by SADC in this context would not bind its member states as is the case in the EU. The fact that the body making the law consists of representatives of member states should not matter as long as the member states themselves intend the laws made to be binding on them. Therefore, SADC member states, by empowering the Summit or other institutions of SADC to legislate on their behalf, have, to some extent limited their sovereignty. For a stronger reason, by establishing a Tribunal with compulsory jurisdiction and power to make binding decisions on matters of SADC law, member states of SADC must clearly have accepted that they are limiting their sovereignty on matters falling within the ambit of SADC.”⁸⁴ However, to date, the Summit has not issued any regulations or directives.

Not all academic commentators agree with this stance. Ndulo states that, “the approach in SADC can be contrasted with that of the European Union. The European Union did not sign the EU Treaty simply to create mutual obligations governed by the law of nations. Rather, they limited their sovereign rights by transferring them to institutions over which they had no direct control. [...] This they created a ‘supranational’ body as opposed to an international body of law and institutions which stood above the individual member states. In contrast, the SADC treaty does not create supranational organs. For instance, SADC organs do not have the power to legislate or issue directives binding on member states. As such, implementation of the relevant objectives, depends entirely on individual member states.”⁸⁵

Article 22 of the Treaty places a duty on Member States who are represented in the Summit to adopt legal instruments for the implementation of the provisions of the Treaty. In his paper *The Role of SADC Institutions in Implementing SDC Treaty Provisions Dealing with Regional Integration* Saurombe notes that, “The SADC Treaty does not state if the binding decisions of the Summit have a direct effect in the territory of Member States. The silence on the part of the SADC Treaty create a gap in the quest for regional integration in the SADC because the manner in which decisions of the Summit are implemented is left to the discretion of Member States.” Further, “it is notable from Articles 10(8), 11(3)(6) and 13(6) that the Summit and other subsidiary organs make decisions by consensus and yet there are no provisions in the Treaty for breaking the impasse where consensus cannot be reached.” Quoting from Erasmus, Saurombe notes further that, in order to reach consensus, decisions are clouded in value formulations and wide discretions that undermine legal certainty and are, in face, anathema to rules-based trade.⁸⁶

2.1.2 The Council of Ministers

As set out in Article 11 of the SADC Treaty, the Council consists of one minister from each Member State, preferably a minister responsible for foreign or external affairs. The Council performs supervisory, executive

⁸⁴ Zenda F “The SADC Tribunal and the Judicial Settlement of International Disputes” Degree Doctor of Laws University of South Africa (2010) 46.

⁸⁵ Ndulo M “African Integrated Schemes: A Case Study of the Southern African Development Community” (1999) *Cornell Law Faculty Publications Paper* 58 18.

⁸⁶ Erasmus G “Is the SADC Trade Regime a Rule-Based System” (2011) *SADC Law Journal* 19.

and advisory functions under the overall supervision of the Summit. Executive functions of the Council include the approval of policies, strategies and programmes, directing, coordinating and supervising the operations of subordinate SADC institutions, determining terms and conditions of SADC staff, developing the SADC common agenda and performing other duties assigned to it by the Summit or the Treaty. As per Article 10(3), the Council can exercise legislative powers if such power is delegated to it.

2.1.3 The Integrated Committee of Ministers

The Integrated Committee of Ministers (ICM) was introduced by the 2001 amendments to the Treaty to take over functions that were previously performed by the various SADC sectors located in each member state. As a result of the restructuring of SADC institutions, all those various sectors in the respective areas of cooperation are now centralised in the form of directorates located at the SADC headquarters in Gaborone, Botswana.⁸⁷

2.1.4 The Standing Committee of Officials (SCO)

The Standing Committee of Officials (SCO) is a technical advisory committee to the Council of Ministers. The SCO meets twice a year. It consists of one Permanent/Principal Secretary, or an official of equivalent rank from each Member State, preferably from a ministry responsible for economic planning or finance. The Chairperson and Vice-Chairperson of the Standing Committee are appointed from the Member States holding the Chairpersonship and Vice-Chairpersonship, of the Council.⁸⁸

2.1.5 The Secretariat

The SADC Secretariat is the Principal Executive Institution of SADC. The Secretariat is responsible for strategic planning and the facilitation and co-ordination and management of all SADC Programmes. It is headed by the SADC Executive Secretary and is located in Gaborone, Botswana.

2.1.6 The Summit Troika

As noted on the SADC website, "SADC Organ on Politics Defense and Security is managed on a Troika basis and is responsible for promoting peace and security in the SADC region. It is mandated to steer and provide Member states with direction regarding matters that threaten peace, security and stability in the region. It is coordinated at the level of Summit, consisting of a Chairperson, Incoming Chairperson and Outgoing Chairperson, and reports to the SADC Summit Chairperson. The SADC Summit and Organ Troika Summit are mutually exclusive; and, the Chairperson of the Organ does not simultaneously hold the Chair of the Summit. The Organ structure, operations and functions are regulated by the Protocol on Politics, Defense and Security Cooperation. Like the Summit chair, the Organ chair rotates on an annual basis.

2.1.7 The Committee of Central Bank Governors

⁸⁷ Zenda *The SADC Tribunal and the Judicial Settlement of International Disputes* 54.

⁸⁸ See <http://www.sadc.int/about-sadc/sadc-institutions/standing-committee-senior>

The Committee of Central Bank Governors (CCBG) was established with the support of the SADC Ministers responsible for national financial matters in July 1995 and approved by SADC Council at their meeting in August 1995. As noted on the CCBG website, “the main reason for establishment of this committee was the need for a specialised body in SADC to promote and achieve closer co-operation among central banks within the Community. Central banks play a crucial role in particular in the promotion of financial and economic development, by way of pursuing policies that enhance financial and macroeconomic stability. The CCBG consists of 15 Governors from the SADC central banks. The CCBG deals with the development of financial institutions and markets, co-operation regarding international and regional financial relations, and monetary, investment and foreign exchange policies. The Governor of the South African Reserve Bank is the Chairperson of the CCBG. The CCBG Secretariat is hosted by the South African Reserve Bank.”⁸⁹

2.1.8 The Tribunal

The SADC Tribunal was established by Article 16 of the Treaty. Its composition jurisdiction and other matters are provided for in the Protocol of the Tribunal. In terms of Article 16(1), the Tribunal, “shall be constituted to ensure adherence to and the proper interpretation of the provisions of this Treaty and subsidiary instruments and to adjudicate upon such disputes as may be referred to it.” Article 16(5) specifically states that, “the decisions of the Tribunal shall be final and binding.” A decision to suspend the Tribunal was taken at the 2010 Windhoek Summit. As noted by Saurombe, “the 2011 Summit put in place a further moratorium barring the Tribunal from accepting any new cases, even those not related to the Campbell case. The Summit also paralysed the Tribunal by not renewing contracts for sitting judges or replacing them. Thus the Tribunal would be unable to accept new cases since it did not comply with the requirements for its composition as prescribed by Article 3 of the SADC Tribunal Protocol.”⁹⁰

2.1.9 The SADC Parliamentary Forum

The SADC Parliamentary Forum (SADC PF) was established as an autonomous institution of SADC in September 1997. The SADC PF was established under the mandate provided in Article 9(1) of the Treaty that provides that other institutions may be established as necessary. As noted by Musavenga, “nowhere near being an integral institution in SADC, and deprived of the power to make decisions that are binding on its own membership (national parliaments), let alone governments and SADC institutions, the SADC PF remains outside the regional policy making arena of SADC. Had the SADC PF been an integral organ of SADC, it would have been on par with the (judiciary) – the Tribunal. The executive branch (Council) would be expected to account to the legislature for regional policy implementation. Consequently, the SADC PF has played a ‘marginal role in the formal integration agenda of SADC as encapsulated in both RISDP and the [Strategic Indicative Plan for the Organ] SIPO, essentially dominated by powerful political executives (Matlosa 2006:18).”⁹¹ It is important to note that since its existence, the SADC PF has not been able to exercise the

⁸⁹ See <https://www.sadcbankers.org/Pages/default.aspx>

⁹⁰ It is noted on the SADC website that, “After several judgements ruling against the Zimbabwean government, the Tribunal was *de facto* suspended at the 2010 SADC Summit. On 17 August 2012 in Maputo, Mozambique, the SADC Summit addressed the issue of the suspended SADC Tribunal. The SADC Summit resolved that a new Tribunal should be negotiated and that its mandate should be confined to interpretation of the SADC Treaty and Protocols relating to disputes between Member States.”

⁹¹ Musavenga *The Proposed SADC Parliament: Old Wine in New Bottles or an Ideal Whose Time Has Come?* 14 notes further that, “the role of national and other parliaments in SADC matters is not contemplated or articulated in any of the policy

functions and powers that are usually associated with formal parliaments.⁹² In November 2008, the SADC PF adopted a Model Law on HIV and AIDS. This Model Law provides a framework for the review and reform of national legislation and its conformity with international human rights law. However, as noted by Musavenga, “like the regional electoral norms and standards developed before it, though highly instructive, the SADC PF’s Model Law does not have the status of soft law to inform policy making in Southern Africa. This is because it was developed by the SADC PF and not one of the structures of SADC fully mandated to do so by the SADC Treaty. Similarly, the SADC PF cannot use the Model Law or electoral norms to hold SADC Member States accountable for lack of compliance.”⁹³

2.2 Legal Status of SADC Instruments

2.2.1 The SADC Treaty and Protocols

The SADC Treaty sets out the main objectives of SADC, namely, to achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the peoples of Southern Africa and support the socially disadvantaged through regional integration. These objectives are to be achieved through increased regional integration, built on democratic principles, and equitable and sustainable development.⁹⁴

Within the SADC framework, only the SADC Treaty and SADC Protocols (and their annexes) are legally binding. This means that they are subject to ratification in accordance with member states’ constitutional provisions and are subject to domestication. Other SADC member states have the right to insist on compliance. Failure to comply amounts to a breach of international law and this can result in serious consequences. In order for a Protocol to enter in to force, two thirds of the Member States need to ratify or sign the agreement, giving formal consent and making the document officially valid. Any Member State that had not initially become party to a Protocol can accede to it at a later stage.

As noted by Zongew, “Article 6(5) of the SADC Treaty places a duty on all member states to accord the SADC Treaty the force of national law. It is however not yet clear whether the Treaty must prevail over national laws in case of conflict between the Treaty and national laws. SADC legislation is binding only on the states that are party thereto and, once ratified or acceded to, does not allow for any reservations by the ratifying state. A member state may withdraw from SADC by serving a written notice of its intention a year in advance to the Chair of SADC, who must inform other member states accordingly. SADC law also comprises non-binding legal instruments, such as model laws and memoranda of understanding (MOU). The Treaty and its protocols are the two primary formal sources of SADC law. The Regional Indicative Strategic Development Plan (RISDP) is the framework for the regional integration of SADC. It is not legally binding but it is highly persuasive and enjoys considerable political legitimacy. Other sources include international law and resolutions of SADC.”⁹⁵

documents of SADC. The closest that one comes to finding an inkling of a parliamentary decision in SADC matters is Article 16(A) of the SADC Treaty.”

⁹² Musavenga, quoting Oosthuizen notes further that, “Far from being known for legislative oversight, the SADC PF is perhaps best known for its observations of elections, its setting of election standards and its efforts to enhance the participation of women in national parliaments (Oosthuizen 2006:189).”

⁹³ Musavenga *The Proposed SADC Parliament: Old Wine in New Bottles or an Ideal Whose Time Has Come?* 24.

⁹⁴ See <http://www.sadc.int/about-sadc/overview/history-and-treaty>

⁹⁵ See Zongwe D 2011 *An Introduction to the Law of the Southern African Development Community*.

2.2.2 SADC Model Laws

Model Laws are legislative texts recommended to Member States for enactment as part of each country's domestic law. As noted by Faira, "a model law is an appropriate vehicle for modernisation and unification of national laws when it is expected that States will wish or need to make adjustments to the text of the model to accommodate local requirements that vary from system to system, or where strict uniformity is not necessary. It is precisely this flexibility that makes model laws easier to negotiate than a text containing obligations that cannot be altered and promotes greater acceptance of a model law than of a convention dealing with the same subject matter."⁹⁶

Several SADC Protocols including the Protocol of Finance and Investment require State Parties to create Model Laws for the Region. Article 2 of Annex 5 of the Protocol on Finance and Investment requires State Parties to "promote the mutual co-operation, co-ordination and harmonisation of the legal and operational frameworks of Central Banks which shall culminate in the creation of a Model Central Bank Statute for the Region as contemplated by the RISDP."⁹⁷ Likewise Annex 6, Co-operation on Payment, Clearing and Settlement Systems, whilst not specifically referring to the creation of a Model National Payment System Law does state in article 6(1)(c) that, the SADC Payment System Steering Committee shall consider and recommend the enactment of, or amendments to, legislation of State Parties relating to payment systems, clearing systems and settlement systems, including the making and amendment of rules and procedures, risk management policies and any other matters relevant to such legislation and such payment systems, clearing systems and settlement systems.⁹⁸

Model Laws are by their very nature, "soft laws" and are not legally enforceable. They are however generally used to guide governments in the crafting and amendment of their own domestic laws. Model Laws are primarily aimed at assisting member states, in particular policy makers and legislative drafters to address all the relevant areas in need of legislative reform without usurping the authority of national legislatures.

2.2.3 The Legal Status of MOU's and TA's

SADC member states often sign Memorandums of Understanding (MOUs) and Technical Agreements (TAs). MOUs and TAs are typically entered into as a non-binding preliminary document that provides a framework for cooperation prior to concluding a binding protocol.⁹⁹ MOU undertakings are referred to as "soft". This means that the provisions contained therein are not legally binding and are merely persuasive. Member states cannot be punished for a failure to comply and such failure does not amount to a breach of international law. The MOU among Member Governments of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) enjoins its members to develop and implement appropriate national anti-money laundering and combating financing of terrorism legislation in the respective countries in accordance with international anti-money laundering and combating financing of terrorism standards.

⁹⁶ Faira *Legal Harmonisation Through Model Laws: The Experience of the United Nations Commission on International Trade Law (UNCITRAL)* (Undated).

⁹⁷ Article 3(d) of Annex 5 reads, "the objectives of this Annex are to: provide the framework for the creation of a Model Central Bank Statute which shall be considered and approved by the Ministers responsible for national financial matters."

⁹⁸ The draft National Payment System Model Law that was drafted several years ago is currently under consideration for review.

⁹⁹ The MOU on Microeconomic Convergence preceded the Protocol on Trade. SADC Declarations are also adopted as antecedents to protocols. The SADC Declaration on Gender led to the SADC Protocol on Gender.

2.3 The Basis for Harmonisation of Payment System Law in SADC

The legal basis for the harmonisation of Payment System Law in the SADC region is found in the Protocol on Finance and Investment (FIP). Article 2(1) states that the Protocol seeks to foster harmonisation of the financial and investment policies of the State Parties in order to make them consistent with objectives of SADC and ensure that any changes to financial and investment policies in one State Party do not necessitate undesirable adjustments in other State Parties. Article 2(2) states that the objective referred to in Article 2(1) is to be achieved through facilitation of regional integration, co-operation and co-ordination within finance and investment sectors with the aim of diversifying and expanding the productive sectors of the economy, and enhancing trade in the Region to achieve sustainable economic development and growth and eradication of poverty by:

- Establishing principles which will facilitate the creation of a coherent and convergent status in the legal and operational frameworks of Central Banks (Article 2(2)(e));
- **Establishing a framework for co-operation and co-ordination between (amongst) Central Banks on payment, clearing and settlement systems (Article 2(2)(f));**
- Co-operating in the area of information technology and communications technology amongst Central Banks (Article 2(2)(g));
- Co-operating on bank supervision amongst Central Banks (Article 2(2)(h));
- Facilitating the development of capital markets in the Region (Article 2(2)(k));
- Co-operating in the area of SADC Stock Exchanges (Article 2(2)(l));
- Co-operating with regard to anti-money laundering issues amongst State Parties (Article 2(2)(m)).

2.3.1 Annex 6 of the Protocol on Financial and Investment (FIP)

Annex 6 of the FIP specifically covers co-operation on Payment Clearing and Settlement Systems. Article 2(1) of Annex 6 states that State Parties agree that the application of Annex 6 is intended to culminate in **convergent national payment system features, policies, practices, rules and procedures within the Region**. In terms of Article 3 of Annex 6 clearly states that the objectives of the Annex are to establish a framework for co-operation and coordination between Central Banks on payment, clearing and settlement systems in order to:

- Define and implement, in each State Party, a safe and efficient payment system based on internationally accepted principles (Article 3(a) of Annex 6);
- Define and implement a cross-border payment strategy for the Region (Article 3(b) of Annex 6);
- Identify, measure, minimise and manage payment system risk (in particular systemic risk relating to payment systems) (Article 3(c) of Annex 6);
- Achieve convergence across the Region of the features, policies, practices, rules and procedures relating to payment systems, clearing system and settlement system (Article 3(d) of Annex 6);
- Conduct ongoing payment system oversight aimed at reducing and eliminating cross-border settlement risk and systemic financial risk (Article 3(e) of Annex 6).

While Annex 6 does not specifically mandate the adoption of a minimum or maximum harmonisation approach or the adoption of a SADC Payment System Model Law, the wording of Article 3(d) of Annex 6, namely, “achieve convergence across the Region of the features, policies, practices, rules and procedures relating to payment systems, clearing system and settlement system” seems to be an indication of the vague notion of harmonisation and to imply that a certain level of harmonisation is sought even if the words, “harmonise

payment system law across the SADC region” are not expressly included in the Annex. This can be contrasted with Article 95 of the EC Treaty that functions as a legal basis for the harmonisation of laws, regulations, and administrative provisions of Member States for the achieving of the internal market.¹⁰⁰

2.3.2 Annex 12 of the Protocol on Financial and Investment (FIP)

Annex 12 on Anti-Money Laundering was added to the Protocol of Finance and Investment in 2012. The preamble to Annex 12 states that, “harmonisation of key aspects of relevant laws and policies will increase the effectiveness of the measures taken by State Parties to address money laundering and financing of terrorism in the region and support finance and investment.” Further, that “harmonisation of key aspects of the relevant laws and policies will create an enabling environment for increased access to financial services in the region, minimise compliance costs for affected Regulated Institutions that operate cross-border in the region and lessen the danger that criminal acts will be displaced from one State Party to another. It is important to note that the preamble also affirms the importance of the full implementation of the Financial Action Task Force (FATF) Recommendations and that any action undertaken by SADC in this area should be consistent with other actions undertaken in other international forums.

Article 3 of Annex 12 specifically states that “each State Party agrees that it will adopt and maintain, in accordance with the FATF Recommendations, measures that are effective and proportionate to combat money laundering and financing of terrorism and that it will do so cognisant of the impact that such measures may have, at national and regional level on:

- (a) crime;
- (b) financial regulation and the regulation of affected businesses and professions;
- (c) access to financial services by low-income persons;
- (d) the management by Regulated Institutions of their duties to comply; and
- (e) the institutional framework for the implementation of the measures including law enforcement, policy-makers and supervisory authorities.”

Article 6 of Annex 12 is particularly relevant as it requires State Parties to “establish preventative measures such as customer due diligence, record keeping, reporting of information and internal compliance measures in accordance with FATF recommendations.” Although the Annex does not promote the establishment of a SADC Model AML/CFT Law, article 6(1) does state that, “regional coordination will promote efficiency and promote arbitrage between State Parties.” The adoption of a risk-based approach is mandated in article 6(2) of Annex 12 that reads:

“State Parties shall create a framework conducive to the risk-based approach for Regulated institutions to comply with the relevant standards set out in the Recommendations and, in particular, that will require them to implement enhanced due diligence measures in respect of high risk transactions and clients while allowing them to apply simplified due diligence measures relating to low risk transactions and clients.”

¹⁰⁰ Article 95(1) of the EC Treaty reads, “by way of derogation from Article 94 and save where otherwise provided in this Treaty, the following provisions shall apply for the achievement of the objectives set out in Article 14. The Council shall, acting in accordance with the procedure referred to in Article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.”

2.3.3 The Cooperation Framework Annex 6 of the FIP

In order to achieve the objectives set out in Article 3 of Annex 6, the Central Bank in each State Party is mandated in terms of Article 4 of Annex 6, in co-operation with the other Central Banks in the Region, to:

- Sensitise the key stakeholders in that State Party to payment system issues (Article 4(1)(a));
- Build payment system capacity in that State Party (Article 4(1)(b));
- Identify and measure payment system risk in that State Party, and establish appropriate procedures for the management of such risk (Article 4(1)(c));
- Develop a legal framework in that State Party to support modern payment system mechanisms (Article 4(1)(d));
- Monitor, on an ongoing basis, international payment system best practices and align the payment system developments in that State Party in accordance therewith (Article 4(1)(e)); and
- Define and implement a payment system strategy in that State Party (Article 4(1)(f)).

The wording of Article 4(1)(d) of Annex 6 is interesting in that it seems to support each sovereign Member States right to develop its own national legal framework to support modern payment system mechanisms without mandating that the legal frameworks in the region should be harmonised. This could, in the long run, be a potential stumbling block to full regional integration and the harmonisation of payment system law and regulation across the SADC region.

Central Banks in each Member State are also mandated to co-operate with each other to:

- Define and implement a cross-border payment strategy for the Region, which strategy may be based on currency convertibility within the Region or, in the future, on a single currency for the Region (Article 4(2)(a));
- Identify and measure payment systems risk and establish appropriate procedures for the management of such risk (Article 4(2)(b));
- Establish and maintain mutually beneficial relationships with international bodies such as the World Bank, the BIS and the central banks of third States (Article 4(2)(c)); and
- Keep abreast of modern trends in payment, clearing and settlement systems (Article 4(2)(d)).

The institutional arrangements specified in Annex 6 of the FIP are set out in Article 5. Through the forum of the CCBG, Central Banks have established a SADC Payment System Steering Committee which is responsible for the implementation of the Annex. As required by Article 5(3), the SADC Payment System Steering Committee has established a SADC Payment System Working Group. The SADC Payment System Steering Committee has delegated the day-to-day administration relating to the implementation of Annex 5 to the SADC Payment System Working Group.

The functions of the SADC Payment System Steering Committee and the Working Group are set out in Article 6 of Annex 5. In particular, the SADC Payment System Steering Committee is tasked with considering and recommending the enactment of, or amendments to, legislation of State Parties relating to the payment system, clearing system and settlement system, including the making and amendment of rules and procedures, risk management policies and any other matters relevant to such legislation and such payment system, clearing system and settlement systems (Article 6(1)(c)). Additionally, in terms of Article 6(1)(g), the SADC Payment System Steering Committee is mandated to establish a payment system oversight function for the Region (Article 6(1)(g)) and is required to keep the CCBG informed of the development and progress in achieving the objectives set out in Article 3. The SADC Payment System Working Group on the other hand is tasked with *inter*

alia, working towards achieving the objectives set out in Article 3 (Article 6(2)(a)) and accomplishing the tasks delegated to it by the SADC Payment System Steering Committee (Article 6(2)(b)).

2.3.4 Institutional Challenges – Annex 12 of the FIP

Article 9(3) of Annex 12 of the FIP reads, 'The State Parties hereby establish the SADC Anti-Money Laundering Committee consisting of one representative and one alternative representative of each national committee established or designated under Article 9(1). The objectives of the SADC Anti-Money Laundering Committee are to (a) review and monitor the implementation of the Annex; and (b) to advise State Parties on additional measures that may further the objectives of the Annex.'¹⁰¹ As per Article 9(6) of Annex 12, in its activities, the SADC Anti-Money Laundering Committee is required to cooperate with ESAAMLG and any other FATF-style regional bodies with State Parties as members and prevent unnecessary duplication of activities.

In theory, Article 9(3) of Annex 12 of the FIP establishes the SADC Anti-Money Laundering Committee. In practice however, this Committee has not been constituted and is therefore not, at this point in time, an official SADC structure. As such, the concern is expressed that the consideration of the information contained in this report and the implementation of both country and SADC wide recommendations may be undertaken by individual countries in an un-coordinated manner. This approach, by its very nature may result in substantially different interpretations of the flexibility provided by the revised FATF Recommendations and will not ensure that the AML/CFT laws and regulations of the SADC countries are harmonised and calibrated.

In order to move towards the defined level of harmonisation and not to be delayed by institutional matters, it is recommended that each SADC country be encouraged and guided by a duly mandated existing SADC structure, potentially the CCBG Legal-Sub Committee or the SADC Payment Steering Committee as duly mandated by the CCBG, to obtain a defined level of legislation and regulation at a national level in line with the revised FATF Recommendations 2012.

Over the longer term, it will however be essential that the Anti-Money Laundering Committee as established by Annex 12 of the FIP is actually constituted, that a chair is appointed and the Committee be formally tasked with carrying the harmonisation work forward. This committee, once constituted will have a vital role to play in ensuring that SADC Member States make appropriate amendment to their domestic laws and regulations, to define the strategic direction to achieve the objectives of Annex 12 and to initiate further research and other projects that will support State Parties in fulfilling these objectives.

2.4 Prior Considerations Before Embarking Upon Harmonisation of Payment System Law

2.4.1 Differing Legal Traditions

At the outset of conducting this comparative review, it is important to note that the differences in legal traditions followed by each SADC country. As noted by Oppong, "a key interstate relational issue in economic integration is how to overcome the challenges posed by differences in national legal traditions and laws. These differences, which exist in substantive and procedural laws, may even extend to legal culture and mode of legal

¹⁰¹ Articles 9(4)(a) and (b) Annex 12.

thought. In Africa, differences in national laws are attributable to the diversity of legal traditions, namely common law, civil law, Roman Dutch law, customary law and Islamic law. The legal traditions of the former colonisers of Africa still prevail in their former colonies. The extent to which these laws vary from country to country in Africa should not be exaggerated. Geographic proximity, common colonial experience and the legislative draftsman's penchant to copy legislation from neighboring countries have led to a situation where, as between countries adhering to the same legal tradition, their laws are very similar. A Ghanaian lawyer that moves to Nigeria will not be bewildered by the principles of the Nigerian legal system. Nor will a Namibian lawyer who moves to South Africa. The same cannot be said for a Ghanaian lawyer who moves to South Africa. This presents advantages and challenges for Africa's economic integration. Differences in national laws are manifest in many areas of law."¹⁰²

When reviewing the current laws and regulations in force in each SADC country, it is important to note the several fundamental differences between common law and civil law traditions. As noted by Tetley, differences are clearly evident the function of jurisprudence, the *stare decisis* doctrine¹⁰³ (unknown in civil law traditions), the style in which judgments are written, the function of statutes, the style of drafting of laws, the interpretation of laws, the concept of the legal rule, categories of laws and rights versus remedies. Most notably, and of fundamental importance to the analysis contained in this report, the style of drafting law is very different in common law and civil law traditions. Common law statutes provide detailed definitions, and each specific rule sets out lengthy enumerations of specific applications or exceptions, preceded by a catch-all phrase and followed by a demurrer such as "notwithstanding the generality of the foregoing." Civil law codes and statutes on the other hand, are concise (*le style français*), provide no definitions, and state principles in broad, general phrases. Additionally, while most common law rules can be changed from time to time, subject to the doctrine of *stare decisis*, civil law principles are often frozen into codes and rigid doctrines, imposed on courts. Common law systems are also considered to be more "open", in the sense that new rules may be created or imported for new facts whereas civil law systems are "closed", in the sense that every possible situation is governed by a limited number of general principles.¹⁰⁴

Angola and the Democratic Republic of the Congo (DRC) follow a strict civil law system based on Portuguese civil law and Belgian version of French civil law respectively. In Mozambique, whilst the Portuguese civil law influence is very strong, the country follows a mixed legal system of Portuguese civil law and customary law. Mauritius has a civil legal system based on French civil law with some elements of English common law. Botswana has a mixed legal system of civil law influenced by the Roman-Dutch model but also applies customary and common law. Several countries have mixed legal systems consisting of English common law, Roman-Dutch civil law, and customary law.

These differences are summarised in Table 1 below and must be taken into consideration when reviewing the current legal and regulatory framework in each country and proposing harmonisation measures in the future.

¹⁰² Oppong, R 2011 *Legal Aspects of Economic Integration in Africa* 106.

¹⁰³ See Tetley S 1999 *Mixed Jurisdictions : Common Law vs Civil Law (Codified and Un-codified) (Part I)* where it is noted that, "the English doctrine of *stare decisis* compels lower courts to follow decisions rendered in higher courts, hence establishing an order of priority of sources by reason of authority. *Stare decisis* is unknown to civil law, where judgments rendered by judges only enjoy the authority of reason."

¹⁰⁴ Tetley *Mixed Jurisdictions : Common Law vs Civil Law (Codified and Un-codified) (Part I)*.

Table 1: Legal Traditions in SADC Countries

Country	Language	Legal Tradition
Angola	Portuguese	Civil legal system based on Portuguese civil law; no judicial review of legislation.
Botswana	English	Mixed legal system of civil law influenced by the Roman-Dutch model and also customary and common law.
DRC	French	Civil legal system based on the Belgian version of French civil law. The DRC is also the only SADC member that is a signatory to the OHADA Treaty and has therefore adopted the OHADA Uniform Acts. ¹⁰⁵
Lesotho	English	Mixed legal system of English common law and Roman-Dutch law; judicial review of legislative acts in High Court and Court of Appeal.
Malawi	English	Mixed legal system of English common law and customary law; judicial review of legislative acts in the Supreme Court of Appeal.
Mauritius	English/French	Civil legal system based on French civil law with some elements of English common law
Mozambique	Portuguese	Mixed legal system of Portuguese civil law and customary law.
Namibia	English	Mixed legal system of un-codified civil law based on Roman-Dutch law and customary law.
Seychelles	English/French	Mixed legal system of English common law, French civil law, and customary law.
South Africa	English	Mixed legal system of Roman-Dutch civil law, English common law, and customary law.
Swaziland	English	Mixed legal system of civil, common, and customary law.
Tanzania	English	English common law; judicial review of legislative acts limited to matters of interpretation.
Zambia	English	Mixed legal system of English common law and customary law; judicial review of legislative acts in an ad hoc constitutional council.
Zimbabwe	English	Mixed legal system of English common law, Roman-Dutch civil law, and customary law.

2.4.2 Different Regulatory Models Applied by SADC Member States

Several different regulatory models are applied in SADC. With respect to the evolution of regulatory models, Volker notes that, "most countries start off with no formal regulation, as the electronic payments environment might still be in its infancy and with low levels of complexity and risk. Generally there is a natural progression to bi-lateral arrangements between the participants – resulting in an ad hoc self-regulatory payments industry. Eventually, as the payment system matures and becomes critical to the effective functioning of the national economy, legislation is introduced to enable more formalised regulation."¹⁰⁶ There are primarily four

¹⁰⁵ OHADA is a system of business laws and implementing institutions adopted by West and Central African nations. OHADA is the French acronym for "Organisation pour l'Harmonisation en Afrique du Droit des Affaires", which translates into English as "Organisation for the Harmonisation of Business Law in Africa". It was created on October 17, 1993 in Port Louis, Mauritius.

¹⁰⁶ Volker *Essential Guide to Payments An Overview of the Services, Regulation and Inner Workings of the South African National Payment System* 267.

approaches to the regulation of a national payment system. These are direct regulation, delegated regulation, self-regulation and no regulation (see Table 2 below).

Table 2: Regulatory Models

Regulatory Models	Description
Direct Regulation	<ul style="list-style-type: none"> • Direct oversight by the Central Bank or other government mandated authority • Empowering legislation includes Central Bank Law, Banking Law, National Payment System Law, Consumer Protection Law, Anti-Money Laundering Law
Delegated Regulation	<ul style="list-style-type: none"> • This is an approach where the ultimate oversight or regulatory authority delegates some or its entire mandate to an industry body to perform the identified roles on its behalf. • Generally the ultimate regulator would retain the right to withdraw the mandate at any time, or to intervene on an ad-hoc basis where necessary. • This is essentially a hybrid between direct and self-regulation.
Self-Regulation	<ul style="list-style-type: none"> • This is the exercise of some degree of regulatory authority over an industry. • Could be applied in addition to some form of government regulation, or it could fill the vacuum of an absence of government oversight and regulation. • The ability of the Self-Regulatory Organisation (SRO) to exercise regulatory authority does not necessarily derive from a grant of authority from the government. Empowering legislation is therefore not always necessary.
No Regulation	<ul style="list-style-type: none"> • Many emerging markets do not have any form of regulation of the national payment system. This creates a vacuum for banks, mobile network operators, IT companies to operate their services as they see fit.

Source: Volker, 2013

Each model has its advantages and disadvantages. For example, while direct regulation has the advantages of maximum enforceability, certainty and long term sustainability, this regulatory model may also stifle innovation, be costly and inefficient and subject to political influence. Where self-regulation allows for greater flexibility and is conducive to innovation, this model may also lead to weaker enforcement, limited powers to sanction and various competition concerns. No regulation on the other hand causes uncertainty, is open to manipulation and in general, leads to inefficiencies.

In the SADC, direct regulation is still the most common regulatory model with the Central Bank at the centre as the designated competent authority (see Table 3 below). Several countries namely Botswana, Seychelles, Swaziland and Zimbabwe apply the direct regulation model but also require that each individual designated and or recognised payment system have a management body or committee, representative of the participants, to organise and manage the system and the participants' participation in it. These management bodies are required to report directly to the Central Bank but must at the same time, have rules and procedures for conducting business that must include inter alia: clearing procedures and clearing times, settlement

arrangements and provision for collateral, agreement on finality of transfers, rules governing the return of items and rules governing management of gridlock.

Table 3: Regulatory Models Applied in SADC

	DIRECT			COMBINATION OF DIRECT & SELF				DIRECT WITH REQUIREMENT THAT EACH SYSTEM HAVE A MANAGEMENT BODY				DIRECT & DELEGATED TO PSMB (Payment Association)		
	Angola	MZ	Zambia	DRC	Malawi	Tanzania	Mauritius	Botswana	Seychelles	Swaziland	Zimbabwe	Lesotho	Namibia	RSA
Direct Regulation	✓	✓	✓	✓	✓	✓	✓					✓	✓	✓
Direct Regulation & Management Body								✓	✓	✓	✓			
Delegated Regulation (PSMB)												✓	✓	✓
Self-Regulation				✓	✓	✓	✓					✓		
No Regulation														

Self-regulation due to no legally enforceable NPS Act.
Self-regulation as NO NPS Act.
Separate legal entity

South Africa, Namibia and Lesotho apply a hybrid or delegated regulatory model. Although the Central Bank in each country is empowered by the National Payments System Act, 1998 (As Amended)¹⁰⁷ (South Africa), the Payment System Management Act, 2003 (As Amended)¹⁰⁸ (Namibia) and the Payment Systems Bill, 2013 (Lesotho) to oversee and regulate the National Payment System, these Acts and in the case of Lesotho the Bill, provide for the recognition of a Payment System Management Body (PSMB) / Payment Association that is mandated amongst other things to organise, manage and regulate in relation to its members, all matters affecting payment instructions. The rules of the PSMB empower that the PSMB to recommend for approval by the Central Bank, criteria subject to which any person is granted membership of the PSMB or is to be authorised to act as a system operator or a Payment Clearing House (PCH) system operator within a payment system and provide for the PSMB to authorise that person to act as a system operator or PCH system operator in accordance with the criteria.

As represented in Table 4 below, when a delegated regulation model is followed, key functions that may or may not be mandated to the Central Bank in other jurisdictions, are delegated to the PSMB. The example provided is drawn from section 4 of the South African National Payments System Act, 1998 (As Amended).¹⁰⁹

¹⁰⁷ Act 78 of 1998 (As Amended).

¹⁰⁸ Act 18 of 2003 (As Amended).

¹⁰⁹ Act 78 of 1998 (As Amended).

Table 4: Functions Delegated to the PSMB in South Africa

Ref.	Function	South African Provision	
S4(1)	Organise, manage and regulate, in relation to its members all matters affecting payment instructions	✓	The objects of the payment system management body are to organise, manage and regulate, in relation to its members, all matters affecting payment instructions.
S4(1)(a)	Provide a forum for the consideration of matters of policy	✓	Provide a forum for the consideration of matters of policy and mutual interest concerning its members.
S4(1)(b)	Act as a medium for communication	✓	Act as a medium for communication by its members with the South African Government, the Reserve Bank, the Registrar of Banks, the Co-operative Bank Supervisors, the Registrar of Financial Institutions, any financial or other exchange, other public bodies, authorities and officials, the news media, the general public and other private associations and institutions.
S4(1)(c)	Deal with matters of interest to members and promote cooperation	✓	Deal with and promote any other matter of interest to its members and to foster co-operation between them.
S4(2)(a)	Admit members & regulate, control & with approval of SARB terminate membership	✓	Rules of the payment system management body must empower that body to admit members and to regulate, control and, with the approval of the Reserve Bank, terminate membership.
S4(2)(b)	Establish or dissolve any body, committee or forum consisting of its members	✓	Rules of the payment system management body must empower that body to constitute, establish or dissolve any body, committee or forum consisting of its members and which has an impact on, interacts with, has access to or makes use of payment, clearing or settlement systems or operations.
S4(2)(c)(i)	Recommend criteria subject to which a person is granted membership of PSMB	✓	Rules of the payment system management body must empower that body to recommend for approval by the Reserve Bank, criteria subject to which any person is granted membership of the payment system management body.
S4(2)(c)(i)	Recommend criteria subject to which a person is to be authorised to act as a system operator or a PCH system operator	✓	Rules of the payment system management body must empower that body to recommend criteria in terms of which a person is to be authorised to act as a system operator or a PCH system operator within a payment system.
S4(2)(c)(ii)	Authorise a person to act as a system operator or PCH system operator	✓	Rules of the payment system management body must empower that body to authorise that person to act as a system operator or PCH system operator in accordance with those criteria.
S4(2)(d)(i) and S4(2)(d)(ii)	Recommend criteria for sponsorship arrangements	✓	Rules of the payment system management body must empower that body to recommend for approval by the Reserve Bank criteria subject to and in accordance with which a member that is also a Reserve Bank settlement system

		<p>participant may be authorised to-</p> <p>(i) allow a bank, a mutual bank, a co-operative bank, a designated clearing system participant or branch of a foreign institution that is not a Reserve Bank settlement system participant to clear; or</p> <p>(ii) clear on behalf of a bank, a mutual bank, a co-operative bank, a designated clearing system participant or a branch of a foreign institution that is not a Reserve Bank settlement system participant: Provided that the member shall settle payment obligations on behalf of such bank, mutual bank, co-operative bank, designated clearing system participant or branch of a foreign institution referred to in subparagraphs (i) and (ii).</p>
--	--	---

Mauritius has elected not to promulgate a National Payment System Act. While the Bank of Mauritius derives regulatory and oversight powers from the Bank of Mauritius Act, 2004,¹¹⁰ several of the key provisions found in other countries National Payment System Acts such as settlement finality and irrevocability and protection from insolvency proceedings are only found in the Mauritius Automated Clearing and Settlement System Participant Procedures, Mauritius Automated Clearing and Settlement System Terms and Conditions and the Port Louis Automated Clearing House Rules, 2013. As such, the model applied in Mauritius is a combination of direct regulation and self-regulation.

The same can be said, at this point in time, in the DRC, Lesotho, Malawi and Tanzania, where the National Payment System Bill has yet to be passed by Parliament. In the absence of a legally enforceable National Payment System Act, participants rely on bi-lateral arrangements between the participants, resulting in an ad hoc self-regulatory payments industry.

2.4.3 Different Levels of Infrastructural Development

The *Principles for Financial Market Infrastructures (PFMI)* report lists five different types of financial market infrastructures (FMIs) that are systemically important. These are payment systems (PS), central securities depositories (CSD), securities settlement systems (SSS), central counterparties (CCP) and trade repositories (TR). It is important to note that the definition of a payment system included in the report distinguishes between retail and large value payment systems.¹¹¹ While there is a presumption that these systems are systemically important, the report notes that national authorities are responsible for determining which systems are systemically important, and as such are expected to observe PFMI principles. The report states further that, “where they exist, statutory definitions of systemic importance may vary somewhat across jurisdictions, but in general a payment system is systemically important if it has the potential to trigger or

¹¹⁰ Act 34 of 2004.

¹¹¹ See Bank for International Settlements and International Organization of Securities Commissions 2012 *Principles for Financial Market Infrastructures* 148, where it is noted that, “payment systems are generally categorised as either a retail payment system or a large-value payment system (LVPS). A retail payment system is a funds transfer system that typically handles a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debits, and card payment transactions. Retail payment systems may be operated either by the private sector or the public sector, using a multilateral deferred net settlement (DNS) or a real-time gross settlement (RTGS) mechanism. An LVPS is a funds transfer system that typically handles large-value and high-priority payments. In contrast to retail systems, many LVPSs are operated by central banks, using an RTGS or equivalent mechanism.”

transmit systemic disruptions; this includes, among other things, systems that are the sole payment system in a country or the principal system in terms of the aggregate value of payments; systems that mainly handle time-critical, high-value payments; and systems that settle payments used to effect settlement in other systemically important FMIs.”

Tables 5 and 6 below list the key systems that have been implemented in each SADC country. There is an assumption that all LVPs, CSDs, SSSs, CCPs, and TRs are systemically important, at least in the jurisdiction where they are located, typically because of their critical roles in the markets they serve. In this regard the *Principles for Financial Market Infrastructures* report notes that, “if an authority determines that a CSD, SSS, CCP or TR in its jurisdiction is not systemically important and, therefore, not subject to the principles, the authority should disclose the name of the FMI and a clear and comprehensive rationale for the determination. Conversely, an authority may disclose the criteria used to identify which FMIs are considered as systemically important and may disclose which FMIs it regards as systemically important against these criteria.”¹¹²

Table 5: FMI Infrastructure in SADC (RTGS)

Country		Date	RTGS System
Angola	✓	2005	<i>Sistema de Pagamentos em Tempo Real (SPTR)</i>
Botswana	✓	2006	Botswana Interbank Settlement System (BISS)
DRC	*	-	<i>The DRC is planning to procure an Automated Transfer System shortly.</i>
Lesotho	✓	2006	Lesotho Wire (LSW)
Malawi	✓	2002	Malawi Interbank Transfers and Settlement System (MITASS)
Mauritius	✓	2000	Mauritius Automated Clearing and Settlement System (MACSS)
Mozambique	✓	2014	<i>Metical em Tempo Real (MTR)</i>
Namibia	✓	2002	Namibia Inter-bank Settlement System (NISS)
Seychelles	*	2014	Preparations to introduce a real-time gross-settlement (RTGS) payment system have commenced. The project is however still in the discussion phase. ¹¹³
South Africa	✓	1998	South African Multiple Option Settlement (SAMOS) System
Swaziland	✓	2007	Swaziland Interbank Payment and Settlement System (SWIPSS)
Tanzania	✓	2004	Tanzania Inter-bank Settlement System (TISS)
Zambia	✓	2004	Zambian Inter-bank Payment and Settlement System (ZIPSS)
Zimbabwe	✓	2002	Zimbabwe Electronic Transfer and Settlement System (ZETSS)

¹¹²

¹¹³ ^{12.} Currently the Central Bank of Seychelles Immediate Transfer Service (CBSITS) is used.

Table 6: FMI Infrastructure in SADC (Other)

Infrastructure	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW
Automated Clearing House (ACH)	✗	✓	*	✓	*	✓	✓	✓	*	✓	✓	✓	✓	✗
Automated Transfer System (ATS)	✗	✗	*	✗	*	✗	✗	✗	✗	✗	✗	✗	✗	✗
National Switch	✗	✗	✗	✗	*	*	✓	✓	✗	✓	✗	✗	✗	✗
Retail Switch(s)	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✓
Securities Settlement System (SSS)	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✓	✗
Central Securities System (CSD)	✗	✓	✗	✓	*	✓	✓	✗	✗	✓	✗	✓	✓	✓
Trade Repository (TR)	✗	✓	✗	✗	✗	✓	✓	*	✗	✓	✗	✗	✓	✗

Table 7: Other Relevant Infrastructure Related Data

	Fixed Broadband Internet Subscribers (per 100 people) ¹¹⁴	Internet Users (per 100 people) ¹¹⁵	Mobile Cellular Subscriptions (per 100 people) ¹¹⁶	Commercial bank branches per 100,000 adults ¹¹⁷	ATMs per 100,000 adults ¹¹⁸
Angola	0.16	16.9	49	11.37	19.10
Botswana	0.78	11.5	150	8.65	26.59
DRC	0.00	1.7	28	0.72	0.67
Lesotho	0.13	4.6	59	3.39	9.17
Malawi	0.01	4.4	28	3.35	4.43
Mauritius	10.57	-	113	21.57	43.62
Mozambique	0.08	4.8	33	3.78	6.90
Namibia	2.78	12.9	103	7.19	47.74
Seychelles	11.72	47.1	159	48.29	51.21
South Africa	2.18	41.0	135	10.42	59.93
Swaziland	0.27	20.8	66	7.09	28.95
Tanzania	0.01	13.1	57	2.21	14.57
Zambia	0.11	13.5	76	4.44	8.58
Zimbabwe	0.55	17.1	97	7.11	4.76

¹¹⁴ World Banks World Development Indicators (2012).

¹¹⁵ World Banks World Development Indicators (2012).

¹¹⁶ World Banks World Development Indicators (2012).

¹¹⁷ International Monetary Fund, Financial Access Survey (2012).

¹¹⁸ International Monetary Fund, Financial Access Survey (2012).

SECTION 3: INTERNATIONAL BEST PRACTICE: CHOICE OF BENCHMARKS

Section 3 of this report provides detailed information on the scope and content of the international soft law standards and hard law benchmarks (EU Regulations and Directives) selected as benchmarks. This information is provided as reference material and should be considered by readers when reading each separate country annexure and the high-level analysis provided in section 4 of this report.

3.1 International Standards (Soft Laws)

Article 4(1)(e) of Annex 6 to the FIP requires each Member State to “monitor, on an ongoing basis, international payment system best practices and align the payment system developments in that State Party in accordance therewith.” Within the payments field, several documents published by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS), the Basle Committee and the Financial Action Task Force (FATF) are recognised as sources of international best practice.¹¹⁹

The Core Principles for Systemically Important Payment Systems (CPSIPS), Recommendations for Securities Settlement Systems (RSSS), Recommendations for Central Counterparties (RCCP), Principles for Financial Market Infrastructures and the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations are all referred to as “soft laws”. International soft laws encompass the whole range of legal norms, principles, codes of conduct and transaction rules of the state practice that are recognised either in formal or informal multilateral agreements. The use of soft law in multilateral agreements generally connotes the consent of the state to apply them but there is no *opinion juris* to make them legally binding as rules of customary international law.¹²⁰

Soft laws, unlike Regulations and Directives issued by the European Union are not legally binding on Member States, they nonetheless create guidelines to deal with certain business exigencies. In this regard, Mugarura notes that, “soft law norms contribute to the development of international rules, standards and legal principles that can as time goes on metamorphose into hard law. It therefore has to be said that countries gain immensely from adopting soft law norms such as the Basle Committee’s Guidelines on Banking Supervision, and the FATF 40+9 recommendations. In a sense, the adoption of soft law norms is driven by the need to have a working framework capable of applying to different countries. In theory, failure to observe soft law does not amount to a breach of international norms, but in practice it may generate some tensions in countries. Jurisdictions that refuse to cooperate and comply with the recommendations of the FATF are publically blacklisted (‘named and shamed’) by FATF and economic sanctions may be imposed against them. When the non-cooperating jurisdiction is a dependency territory, then the blacklisting applies to that territory. In the same respect, the World Bank and the International Monetary Fund have co-opted the Basle and FATF supervisory standards in its monitoring framework for national economies. Therefore, countries seeking to use the World Bank and the Fund’s resources are expected to adjust their national economic systems as a condition for lending.”

Most Central Banks in the SADC region have elected to formally endorse and adopt *the Principles for Financial Market Infrastructures PFMI*s into the regulatory framework for the National Payment System. However, it

¹¹⁹ See Volker *Essential Guide to Payments: An Overview of Services, Regulation and Inner Workings of the South African National Payment System* 268 where the author states that, “the most important organisation relevant to setting standards and guidelines for the appropriate and effective regulation of payment systems is the Bank for International Settlements or the BIS. In order to assist central banks of countries to align their regulation of the payment system with what is considered ‘best practice’, the BIS has from time to time issued relevant principles.”

¹²⁰ See Mugarura *The Mechanisms for Harmonisation of Global Anti-money Laundering Laws: An Institutional Framework* 12.

must be noted that principles are not hard Laws, Regulations or Directives that can be directly transposed into national statutes. As such, several regulators interviewed during the course of the in-country stakeholder interviews conducted during the course of this project noted the difficulty in interpreting, applying and translating the international best practice principles into hard law and regulation.

3.1.1 The CPSIPS and PFMI's

3.1.1.1 Core Principles for Systemically Important Payment Systems (CPSIPS)

The CPSIPS were the first set of internationally recognised standards. Published by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS) in January 2001, the 10 principles for the safe and efficient design and operation of systemically important payment systems have over the years become the *de facto* standard.¹²¹ These principles drew extensively from the Report of the Committee on Interbank Netting Schemes of the central banks of the Group of Ten countries (also known as the Lamfalussy Report), which was published in November 1990. The principles were intended to be broad in scope so as to apply to a wide range of circumstances and to be useful over time. The original ten core principles and four responsibilities of central banks in applying the principles are set out in Table 8 below.

Table 8: Ten Core Principle for Systemically Important Payment Systems and Four Responsibilities of Central Banks in Applying Them

Principle	Detail
I	The system should have a well-founded legal basis under all jurisdictions.
II	The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the financial risks they incur through participation in it.
III	The system should have clearly defined procedures for the management of credit risks and liquidity risks, which specify the respective responsibilities of the system operator and the participants and which provide appropriate incentives to manage and contain those risks.
IV	The system should provide prompt and final settlement on the day of value, preferably during the day and at a minimum at the end of the day.
V	A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participant with the largest single settlement obligation.
VI	Assets used for settlement should preferably be a claim on the central bank; where other assets are used, they should carry little or no credit risk and little or no liquidity risk.
VII	The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing.
VIII	The system should provide a means of making payments which is practical for its users and efficient for the economy.
IX	The system should have objective and publically disclosed criteria for participation, which permit fair and open access.
X	The system's governance arrangements should be effective, accountable and transparent.
Responsibilities of Central Banks	
A	The central bank should define clearly its payment system objectives and should disclose publicly

¹²¹ Bank for International Settlements Committee on Payment and Settlement Systems 2001 *Core Principles for Systemically Important Payment Systems*.

	its role and major policies with respect to systemically important payment systems.
B	The central bank should ensure that the systems it operates comply with the Core Principles.
C	The Central Bank should oversee compliance with the Core Principles by systems it does not operate and should have the ability to carry out this oversight.
D	The central bank, in promoting payments system safety and efficiency through the Core Principles, should cooperate with other central banks and with any other relevant domestic or foreign authorities.

3.1.1.2 Recommendations for Securities Settlement Systems (RSSS)

The CPSIPS were followed by the Recommendations for Securities Settlement Systems (RSSS), which were published jointly by the CPSS and the Technical Committee of the International Organization of Securities Commissions (IOSCO) in November 2001.¹²² This report identified 19 recommendations for promoting the safety and efficiency of securities and settlement systems.

3.1.1.3 Recommendations for Central Counterparties (RCCP)

In November 2004, building upon the recommendations established in the RSSS, the CPSS the Technical Committee of IOSCO published the Recommendations for Central Counterparties (RCCP).¹²³ The RCCP provides 15 recommendations that addressed the major types of risks faced by CCPs.

3.1.1.4 Principles for Financial Market Infrastructures (PFMI)

The Bank for International Settlements and International Organization of Securities Commissions (IOSCO) *Principles for Financial Market Infrastructures (PFMI)* 2012 report replaces the previous three sets of standards set out above.¹²⁴ The new principles are updated, harmonised and strengthened and apply to payment systems (PSs), Central Securities Depositories (CSDs), Securities Settlement Systems (SSSs), Central Counterparties (CCPs) and Trade Repositories (TRs). These standards are principles based in recognition of the fact that financial market infrastructures (FMIs) often have different approaches to achieving a particular result.¹²⁵ The twenty-four principles are complemented by five responsibilities of authorities to provide for the effective

¹²² Bank for International Settlements and International Organization of Securities Commissions 2001 *Recommendations for Securities Settlement Systems*.

¹²³ Bank for International Settlements and International Organization of Securities Commissions 2004 *Recommendations for Central Counterparties*. A central counterparty is defined as, “an entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer.”

¹²⁴ Bank for International Settlements and International Organization of Securities Commissions 2012 *Principles for Financial Market Infrastructures*.

¹²⁵ FMIs are defined as an FMI is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions; See Volker Essential Guide to Payments: An Overview of Services, Regulation and Inner Workings of the South African National Payment System 270 where the author notes further that, “overall the new principles have strengthened risk-management guidance, provided new requirements and broadened the scope and applicability of principles to different types of FMIs, such as TRs. For example, the principles require that certain FMI’s maintain a higher level of financial resources to address credit, liquidity and general business risks than in the past. Equally important, the principles provide greater guidance on governance for an FMI’s operations. Further, the principles provide more-detailed guidance on the risks associated with tiered participation in FMIs and place new emphasis on transparency.”

regulation, supervision and oversight of FMIs. As noted by Volker, “these principles and responsibilities are consistent with the G20 and FSB strategies of cooperation, access and resolution for CCPs.”¹²⁶ The report lists five different types of financial market infrastructures (FMIs) that are systemically important, PS, CSD, SSS, CCP and TRs.

Table 9: General Applicability of Principles to Specific Types of FMIs

	PSs	CSD	SSS	CCP	TRs
General Obligations					
1) Legal basis ¹²⁷	✓	✓	✓	✓	✓
2) Governance ¹²⁸	✓	✓	✓	✓	✓
3) Framework for the comprehensive management of risks ¹²⁹	✓	✓	✓	✓	✓
Credit and Liquidity Risk Management					
4) Credit risk ¹³⁰	✓	✗	✓	✓	✗
5) Collateral ¹³¹	✓	✗	✓	✓	✗
6) Margin ¹³²	✗	✗	✗	✓	✗
7) Liquidity risk ¹³³	✓	✗	✓	✓	✗
Settlement					
8) Settlement finality ¹³⁴	✓	✗	✓	✓	✗
9) Money Settlements ¹³⁵	✓	✗	✓	✓	✗

¹²⁶ Volker *Essential Guide to Payments: An Overview of Services, Regulation and Inner Workings of the South African National Payment System* 271.

¹²⁷ An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

¹²⁸ An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

¹²⁹ An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

¹³⁰ An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence.

¹³¹ An FMI that requires collateral to manage its or its participants’ credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce appropriately conservative haircuts and concentration limits.

¹³² A CCP should cover its credit exposures to its participants for all products through an effective margin system that is risk-based and regularly reviewed.

¹³³ An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.

¹³⁴ An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

¹³⁵ An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.

10) Physical deliveries ¹³⁶	✗	✓	✓	✓	✗
Central Securities Depositories and Exchange-of-value Settlement Systems					
11) Central Securities Depositories ¹³⁷	✗	✓	✗	✗	✗
12) Exchange-of-value Settlement Systems ¹³⁸	✓	✗	✓	✓	✗
Default Management					
13) Participant-default Rules and Procedures ¹³⁹	✓	✓	✓	✓	✗
14) Segregation and portability ¹⁴⁰	✗	✗	✗	✓	✗
General Business and Operational Risk Management					
15) General business risk ¹⁴¹	✓	✓	✓	✓	✓
16) Custody and investment risks ¹⁴²	✓	✓	✓	✓	✗
17) Operational risk ¹⁴³	✓	✓	✓	✓	✓
Access					
18) Access and Participation Requirements ¹⁴⁴	✓	✓	✓	✓	✓
19) Tiered Participation Arrangements ¹⁴⁵	✓	✗	✗	✗	✗
20) FMI links ¹⁴⁶	✗	✓	✓	✓	✓
Efficiency					
21) Efficiency and effectiveness ¹⁴⁷	✓	✓	✓	✓	✓
22) Communication Procedures and Standards ¹⁴⁸	✓	✓	✓	✓	✓

¹³⁶ An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.

¹³⁷ A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimise and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry.

¹³⁸ If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.

¹³⁹ An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

¹⁴⁰ A CCP should have rules and procedures that enable the segregation and portability of positions of a participant's customers and the collateral provided to the CCP with respect to those positions.

¹⁴¹ An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

¹⁴² An FMI should safeguard its own and its participants' assets and minimise the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

¹⁴³ An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

¹⁴⁴ An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

¹⁴⁵ An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

¹⁴⁶ An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

¹⁴⁷ An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

Transparency					
23) Disclosure of Rules, Key Procedures, and Market Data ¹⁴⁹	✓	✓	✓	✓	✓
24) Disclosure of Market Data by Trade Repositories ¹⁵⁰	✗	✗	✗	✗	✓

Responsibilities of central banks, market regulators, and other relevant authorities for financial market infrastructures: The *Principles for Financial Market Infrastructures (PFMI)* report is far more comprehensive than the originally published *Core Principles for Systemically Important Payment Systems (CPSIPS)* report with respect to the roles and responsibilities of central banks, market regulators and other relevant authorities for market infrastructure. The report provides guidance for consistent and effective regulation, supervision, and oversight of FMIs but at the same time cautions that authorities for FMIs should accept and be guided by the responsibilities in the report, but that these should be consistent with relevant national law. These responsibilities listed in the report are consistent with international best practices. The five overarching responsibilities are set out in Table 10 below.

Table 10: Responsibilities of Central Banks, Market Regulators and Other Relevant Authorities

Responsibilities of Central Banks, Market Regulators, and Other Relevant Authorities
<p>A) Regulation, Supervision, and Oversight of FMIs FMIs should be subject to appropriate and effective regulation, supervision, and oversight by a central bank, market regulator, or other relevant authority.</p>
<p>B) Regulatory, Supervisory, and Oversight Powers and Resources Central banks, market regulators, and other relevant authorities should have the powers and resources to carry out effectively their responsibilities in regulating, supervising, and overseeing FMIs.</p>
<p>C) Disclosure of Policies with Respect to FMIs Central banks, market regulators, and other relevant authorities should clearly define and disclose their regulatory, supervisory, and oversight policies with respect to FMIs.</p>
<p>D) Application of the Principles for FMIs Central banks, market regulators, and other relevant authorities should adopt the CPSS-IOSCO Principles for financial market infrastructures and apply them consistently.</p>
<p>E) Cooperation with Other Authorities Central banks, market regulators, and other relevant authorities should cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMIs.</p>

3.1.2 UNCITRAL Model Law on Electronic Commerce (1996)

The United Nations Commission on International Trade Law (UNCITRAL) released the UNCITRAL Law on Electronic Commerce in 1996. This model law has gained significant international acceptance and has been used by several SADC member States as the foundation for their own domestic laws.¹⁵¹

¹⁴⁸ An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

¹⁴⁹ An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

¹⁵⁰ A TR should provide timely and accurate data to relevant authorities and the public in line with their respective needs.

Davidson notes further that the Model Law does not specifically refer to contract law. Instead it deals with the principle of functional equivalence of electronic media in commercial transactions. [This means] that where the electronic form is functionally equivalent to the traditional form, it should be treated equally by the law.¹⁵² This principle permeates all legislation based on the model law. A second principle underlying the Model Law is that of **technology neutrality** (the term was chosen in response to the recognition that technology is constantly developing). For example, as 'electronic mail' connotes a certain medium, the Model Law uses the general expression data message.¹⁵³ The third relevant principle is that of party autonomy. In this regard Faria notes that, "the model law recognises the importance of contract and 'party autonomy.'" On the one hand, its non-mandatory provisions leave the parties free to organize the use of electronic commerce among themselves. On the other hand, some of the Model Law's mandatory provisions allow agreements concluded between the parties to be taken into consideration in assessing whether the nature of the methods used to ensure, for example, the security of messages, is reasonable or appropriate for the purpose."

As set out in Table 11 below, the Model Law addresses the legal recognition of data messages, writing, signatures, originals, admissibility and evidentiary weight of data messages, retention of data messages, the formation and validity of contracts, the recognition by the parties of data messages, attribution of messages, acknowledgement of receipt and the time and place of dispatch and receipt of data messages.¹⁵⁴

Table 11: UNCITRAL Model Law on Electronic Commerce (1996)

Article	Subject	Detail
CHAPTER I GENERAL PROVISIONS		
Article 1	Scope & application	This Law applies to any kind of information in the form of a data message used in the context of commercial activities.
Article 2	Definitions	Data message means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; Electronic data interchange (EDI) means the electronic transfer from computer to computer of information using an agreed standard to structure the information; Originator of a data message means a person by whom, or on whose

¹⁵¹ Except in Europe, where legislation has been primarily influenced by directives issued by the European Union, most countries that have legislated in relation to electronic commerce have used the Model Law on Electronic Commerce as their template.

¹⁵² See Faria *Legal Harmonisation Through Model Laws: The Experience of the United Nations Commission on International Trade Law (UNCITRAL)* where the author notes that the UNCITRAL Model Law is based on three basic principles: functional equivalence; technology neutrality and party autonomy. "The basic assumption of the Model Law is that traditional legal notions (such as 'document' or 'instrument', 'written' contract, 'signed' or 'sealed' record) need not be replaced by entirely new ones. Instead, the Model Law identifies the circumstances under which the same function envisaged by the law for, say, a 'written contract' may be fulfilled by the exchange of communications in electronic form. The approach taken by the Model Law has been called a 'functional equivalence approach.'"

¹⁵³ See Faria *Legal Harmonisation Through Model Laws: The Experience of the United Nations Commission on International Trade Law (UNCITRAL)* where the author notes that, "the rules of the Model Law are 'neutral' rules; that is they do not depend on or presuppose the use of particular types of technology and should be applies to the communication and storage of all types of information, which is particularly important in view of speed of technological innovation and development."

¹⁵⁴ The Model Law on Electronic Commerce was followed in 2001 by the UNCITRAL Model Law on Electronic Signatures. This Model Law deals specifically with issues related to electronic signatures, their legal effect and rules of conduct for parties involved in cross-border issues.

		<p>behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;</p> <p>Addressee of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;</p> <p>Intermediary, with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;</p> <p>Information system means a system for generating, sending, receiving, storing or otherwise processing data messages.</p>
Article 3	Interpretation	<p>(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.</p> <p>(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.</p>
Article 4	Variation by agreement	<p>(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.</p> <p>(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.</p>
CHAPTER II APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES		
Article 5	Legal recognition of data messages	Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.
Article 5 bis	Incorporation by reference ¹⁵⁵	Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.
Article 6	Writing	<p>(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.</p> <p>(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.</p>
Article 7	Signature	<p>(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:</p> <p>(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and</p> <p>(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.</p> <p>(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.</p>

¹⁵⁵ As adopted by the Commission at its thirty-first session, in June 1998.

Article 8	Original	<p>(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:</p> <p>(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and</p> <p>(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.</p> <p>(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.</p> <p>(3) For the purposes of subparagraph (a) of paragraph (1):</p> <p>(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and</p> <p>(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.</p>
Article 9	Admissibility and evidential weight of data messages	<p>(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:</p> <p>(a) on the sole ground that it is a data message; or,</p> <p>(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.</p> <p>(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.</p>
Article 10	Retention of data messages	<p>(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:</p> <p>(a) the information contained therein is accessible so as to be usable for subsequent reference; and</p> <p>(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and</p> <p>(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.</p> <p>(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.</p> <p>(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.</p>

CHAPTER III. COMMUNICATION OF DATA MESSAGES		
Article 11	Formation and validity of contracts	(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.
Article 12	Recognition by parties of data messages	(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.
Article 13	Attribution of data messages	<p>(1) A data message is that of the originator if it was sent by the originator itself.</p> <p>(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:</p> <p>(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or</p> <p>(b) by an information system programmed by, or on behalf of, the originator to operate automatically.</p> <p>(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:</p> <p>(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or</p> <p>(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.</p> <p>(4) Paragraph (3) does not apply:</p> <p>(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or</p> <p>(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.</p> <p>(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.</p> <p>(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew</p>

		or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.
Article 14	Acknowledgement of receipt	<p>(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.</p> <p>(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:</p> <p>(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:</p> <p>(i) at the time when the data message enters the designated information system; or</p> <p>(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;</p> <p>(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.</p> <p>(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).</p> <p>(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:</p> <p>(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business; (b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.</p>

3.1.3 The FATF Recommendations (2012)

Anti-money laundering and counter terrorist financing requirements and regulatory measures are becoming increasingly important to regulators tasked with ensuring the safety, efficiency and security of payment systems, products and distribution channels. The importance of a harmonised AML regulatory framework for SADC is set out in Annex 12 of the SADC Protocol of Finance and Investment. The preamble to Annex 12 states that, "harmonisation of key aspects of relevant laws and policies will increase the effectiveness of the measures taken by State Parties to address money laundering and financing of terrorism in the region and support finance and investment." Further, that "harmonisation of key aspects of the relevant laws and policies will create an enabling environment for increased access to financial services in the region, minimise compliance costs for affected Regulated Institutions that operate cross-border in the region and lessen the danger that criminal acts will be displaced from one State Party to another. It is important to note that the preamble affirms the importance of the full implementation of the Financial Action Task Force (FATF) Recommendations and that any action undertaken by SADC in this area should be consistent with other actions undertaken in other

international forums. Annex 12 of the FIP is legally binding on all signatories. As such, the choice of the FATF Recommendations as the de facto standard for harmonisation of all AML/CFT laws and regulations in the SADC region is mandated.

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse. As explained by FATF,

“the original FATF Recommendations were drawn up in 1990 and revised in 1996 to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT). Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigor in the Recommendations.”¹⁵⁶

The 2012 Recommendations combine the original 40 Recommendations and nine Special Recommendations on Terrorist Financing into 40 consolidated recommendations supported by Interpretive Notes. From a payments perspective, seven of the FATF recommendations are particularly relevant to retail payments and serve as a harmonisation benchmark. These are FATF Recommendation 1) Assessing Risks and Applying the Risk Based Approach; Recommendation 10) Customer Due Diligence; Recommendation 11) Record Keeping; Recommendation 13) Correspondent Banking; Recommendation 14) Money or Value Transfer Services (MVTs); Recommendation 15) New Technologies; Recommendation 16: Wire Transfers and Recommendation 17) Reliance on Third Parties.

3.1.3.1 FATF Recommendation 1: Assessing Risks and Applying the Risk Based Approach

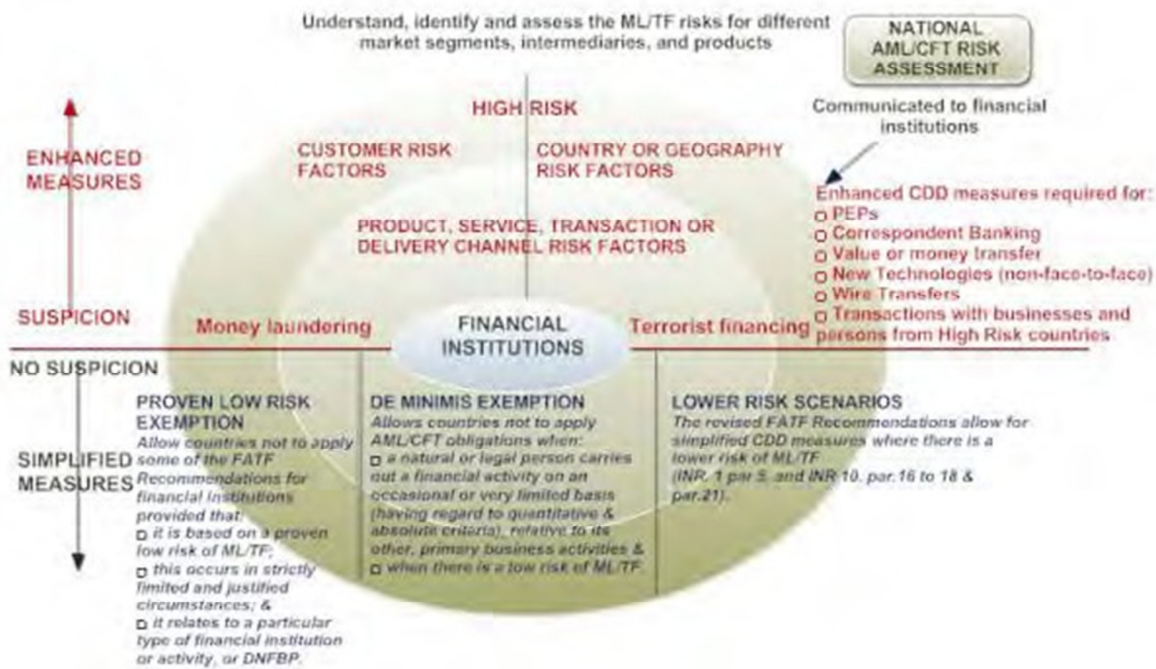
FATF Recommendation 1 requires countries to identify, assess and understand the money laundering and terrorist financing risks for the country and to take action, including the designation of an authority or mechanism to coordinate actions and assess risks. Countries are required to apply a risk based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries are also required to ensure that financial institutions and designated non-financial businesses and professions (DNFBPs) identify, assess and take effective actions to mitigate their money laundering and terrorist financing risks. Importantly, where countries identify higher risks, they must ensure that their AML/CFT regime addresses these risks. Where lower risks are identified, countries are permitted to allow simplified measures for some of the FATF Recommendations.

¹⁵⁶ Financial Action Task Force (FATF) 2012 *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*.

While the FATF has always advocated the RBA, the 2012 FATF Recommendations have catapulted the adoption and implementation of a risk-based approach to the forefront as Recommendation 1 focuses on 'the need to understand, identify and assess risks and to apply mitigation and management measures that are risk-sensitive, through a risk based approach.'¹⁵⁷ The first guidance paper on adopting a risk-based approach was released by FATF in 2007. This paper set out the purpose, benefits and challenges of a risk-based approach, provided guidance to public authorities on creating and implementing a risk based approach and guidance to financial institutions on implementing a risk-based approach. This paper was however based on the 2003 FATF Recommendations, which did not make the risk-based approach central to implementing the FATF Recommendations.

Essentially, the risk-based approach requires countries and financial institutions to take enhanced measures to manage and mitigate risks when these risks are seen as 'higher risk' and gives them the option to adopt simplified measures where risks are lower and there is no suspicion of possible money laundering and terrorist financing activities. The risk-based approach also creates exemptions from certain requirements if there is a proven low risk and certain other requirements are met.

Diagram 2: Risk-Based Approach (The Exemptions)



3.1.3.1.1 The Proven Low Risk Exemption

A FATF, APGM and World Bank report notes that, "the main challenges for countries seeking to make use of the proven low risk exemption will be to demonstrate the limited and justified circumstances pertaining to a specific type of financial institution, Designated Non-Financial Businesses and Professions (DNFBP), or activity and provide justification for the view that there is a low risk of ML and TF. The justification should be based on

¹⁵⁷ 18.

an appropriate risk assessment and the level of detail will depend on the range and possible impact of the exemption."¹⁵⁸

We argue that the wording of FATF Recommendation 10(ii) namely, "Financial institutions should be required to undertake customer due diligence (CDD) measures when, 'carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16,'" amount to proven low risk exemptions and not scenarios in which lower CDD measures may be applied. This is supported by the 'negative' reading of Recommendation 10(ii) read together with Recommendation 16 that would read:

"Financial institutions [are not] required to undertake customer due diligence (CDD) measures when, "carrying out occasional transactions: (i) [below] the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16."

Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

- (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
- (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.'

Therefore, customer due diligence measures for **occasional transactions** below USD/EUR 15,000 and cross-border wire transfers below USD/EUR 1,000 are not required and therefore fall within the Proven Low Risk Exemption envisaged and permitted by FATF Recommendation 10(ii).

Commenting on this permitted exemption, de Koker notes that,

"the FATF differentiates between CDD measures in relation to account-based products and those in relation to occasional (non-account-based) transactions, such as occasional money transfers and many prepaid cards. Recommendation 5 states that no financial institutions should keep anonymous accounts or accounts in obviously fictitious names. Identification and verification measures must therefore be taken in respect of account-based products, irrespective of the value concerned. Occasional transactions, on the other hand, are treated differently. Customers only need to be identified and their particulars verified if the value of the transaction exceeds USD/EUR 15,000 or, in the case of wire transfers, USD/EUR 1,000. This exemption is set out in the Recommendations and countries do not need to argue and prove that they pose a lower risk to justify the exclusion of these transactions from the standard FATF CDD controls."¹⁵⁹

¹⁵⁸ Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank 2013 *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 25.

¹⁵⁹ See de Koker L 2011 *Aligning Anti-Money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when FATF Standards are Clarified* *Journal of Financial Crime*, vol. 18, no. 4 361 where the author submits that, "such a distinction undermines a principled risk-based approach in relation to financial inclusion products. USD/EUR 15,000 is a vast sum from the perspective of low income persons. The majority of low-value financial inclusion accounts that are targeted at the unbanked will not have an amount of USD/EUR 15,000 flowing through them during the

A good example of a Proven Low Risk Exemption is the South African prepaid low value payment product exemption that was issued in 2010.¹⁶⁰ See section J of Annexure J for full details on the South African prepaid low value payment product exemption.

It is noted in the recent FATF guidance paper on prepaid cards, mobile payments and Internet-based payment services that, 'for prepaid cards, the risk posed by anonymity (not identifying the customer) can occur when the card is purchased, registered, loaded, reloaded, or used by the customer. The level of risk posed by anonymity is relative to the functionality of the card and the existence of AML/CFT risk mitigation measures such as funding or purchasing limits, reload limits, cash access, and whether the card can be used outside the country of issue.'¹⁶¹ All of these risk mitigation measures are clearly set out in the South African Prepaid Low Value Payment Product Exemption as follows:

- The value of every transaction initiated through the prepaid instrument cannot exceed R200.00 (USD 19.75);
- the available balance on the prepaid instrument cannot exceed R1500.00 (USD148.11) at any time;
- the monthly turnover of value loaded onto the prepaid instrument cannot exceed R3,000 (USD 296.22) per month;
- the prepaid instrument may only be used domestically in South Africa;
- the prepaid instrument cannot be used for remittances (both domestic and international); and
- the prepaid instrument cannot be used for the withdrawal of cash (at an ATM) or to facilitate cash back as part of a transaction for goods or services.

While the issuers of prepaid card instruments that meet the required criteria are exempt from establishing and verifying the identity of customers and keeping certain records, in order to meet the FATF requirement that there be "a proven low risk of money laundering and terrorist financing", issuers of such prepaid instruments are required to abide by several strict conditions. These include the adoption of enhanced measures over and above normal procedures, scrutinising transactional activity on an ongoing basis with the view to identifying and reporting suspicious transactions. Importantly, if the prepaid cards are issued to a client on behalf of the accountable institution, the accountable institution must establish and verify the identity of the persons issuing the prepaid card on its behalf and applies enhanced measures to scrutinise the transaction activity of the person issuing the prepaid instrument on an on-going basis.

3.1.3.1.2 *The De Minimus Exemption*

The second situation referred to in the FATF Interpretative Note to Recommendation 1, paragraph 6(b), that permits countries not to apply some of the FATF Recommendations is where "a financial activity (other than the transferring of money or value) is carried out by a natural or legal person **on an occasional or very limited basis** (having regard to quantitative and absolute criteria) such that there is low risk of money laundering or

duration of the account. However, in terms of the current scheme of the Recommendations, such accounts must be subjected to appropriate controls and cannot be opened anonymously."

¹⁶⁰ Gazette 33309 No. 560 Financial Intelligence Centre Act (38/2001): Exemptions in terms of the Act (2010) (Prepaid Instruments).

¹⁶¹ Financial Action Task Force (FATF) *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services* 14.

terrorist financing.’ The FATF, APGM and World Bank AML/CFT and Financial Inclusion Guidance report refers to this situation as the so called ‘de minimis exemption.’¹⁶² In this context, ‘de minimis’ means ‘on an occasional and limited basis’ and does not refer to a monetary threshold.

The FATF Recommendations explicitly refer to the words ‘de minimis’ in the FATF Interpretive Note 16, paragraph 5 which reads, ‘countries may adopt a *de minimis threshold* for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

- (a) Countries should ensure that financial institutions include with such transfers:
 - (i) the name of the originator;
 - (ii) the name of the beneficiary; and
 - (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
- (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.’

Here, it appears that FATF are referring to the “**occasional or limited basis**” of the wire transfer as the basis for the use of the words ‘de minimis’ with the additional requirement that the transfer should be below the **threshold** of USD/EUR 1,000. In these circumstances, the application of the principles applicable to the proven low risk exemption as per FATF Interpretive Note 1, paragraph 6(a) and not 6(b), apply. This is supported by the fact that the exemption provided for in Interpretive Note 1, paragraph 6(b) cannot apply to the transferring of money or value and a wire transfer is most certainly the transfer of money or value.

The circumstances under which a financial activity can be defined as occurring on an “occasional or limited basis” is open to interpretation.¹⁶³ As stated in the FATF, APGM and World Bank AML/CFT and Financial Inclusion Guidance report, “countries that opt to apply the de minimis exemption must be able to demonstrate a cause and effect relationship between the very limited and occasional nature of the financial activity and the assessed low level of ML and TF risk. When a country decides to exempt certain natural or legal persons from AML/CFT requirements because they engage in financial activity on an occasional or very limited basis, the onus is on the country to establish that the conditions set out in the FATF Recommendations are met.”¹⁶⁴

A practical example of a ‘de minimis exemption’ as described in the FATF Interpretive Note 1, paragraph 6(b) can be found in the United Kingdom’s Money Laundering Regulations, 2007.¹⁶⁵ In terms of Regulation 4(1)(e), the Regulations do not apply to, ‘a person whose main activity is that of a high value dealer, when he engages in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations.’ The Regulations are also not applicable to, ‘a person who falls within regulation 3 solely as a result of his engaging in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations.’¹⁶⁶

Paragraph 1 of Schedule 2 states that a person is considered as, “engaging in financial activity on an occasional or very limited basis if all the following conditions are fulfilled—

¹⁶² Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 25.

¹⁶³ 25.

¹⁶⁴ 25.
¹⁶⁵ 2007 No. 2157.

¹⁶⁶ Regulation 4(2).

- (a) the person's total annual turnover in respect of the financial activity does not exceed £64,000;
- (b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1,000 euro, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;
- (c) the financial activity does not exceed 5% of the person's total annual turnover;
- (d) the financial activity is ancillary and directly related to the person's main activity;
- (e) the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;
- (f) the person's main activity is not that of a person falling within regulation 3(1)(a) to (f) or (h);
- (g) the financial activity is provided only to customers of the person's main activity and is not offered to the public."

3.1.3.1.3 *The Lower Risk Scenarios*

Contrasted to the exemptions provided for in FATF Interpretative Note 1, paragraph 6(a) and (b), FATF Recommendations 1 and 10 read together with FATF Interpretive Note 1, paragraph 5 and Interpretive Note 10, paragraphs 16 to 18 and 21, permit financial institutions to apply simplified CDD measures where there is a lower risk of money laundering and terrorist financing. What this means is that countries are permitted to allow their financial institutions (in specified circumstances) to apply simplified CDD measures such as only requiring an individual to provide some form of identification and not requiring them to provide proof of address or source of funds. It is important to note that, 'simplified CDD measures never means a complete exemption or absence of CDD measures. A simplified set of CDD measures may be basic and minimal but must still respond to each of the four CDD components that apply to standard customer relationships and transactions.'¹⁶⁷ For a detailed discussion on the four CDD components that apply to standard customer relationships and transactions and the flexibility provided for with respect to simplified CDD measures under certain circumstances.

3.1.3.1.4 *Higher Risk*

At the other end of the spectrum where higher risks are identified, financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks. Enhanced measures are required for Politically Exposed Persons (Recommendation 12), Correspondent Banking (Recommendation 13), Value or Money Transfer Services (Recommendation 14), New Technologies (Recommendation 15), Wire Transfers (Recommendation 16) and transactions with businesses and persons from high risk countries (Recommendation 19). In addition to these FATF designated higher risk customers and activities, FATF requires countries and customers to assess their risks through National AML/CFT Risk Assessments. These country level Assessments may in turn reveal additional higher risk customers and or activities within the specific national context. In February 2013, the FATF released their guidance on National Money laundering and Terrorist Financing Risk Assessments with the objective of providing guidance on the conduct of risk assessment at the country or national level, and it relates especially to key requirements set out in Recommendation 1 and paragraphs 3-6 of INR 1. The guidance recognises that a ML/TF risk assessments may be undertaken at different levels and with differing purposes and scope, including supranational assessments (of a group of countries), national (or country level) assessments and sub-national assessments (of a particular sector, region,

¹⁶⁷ Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 29.

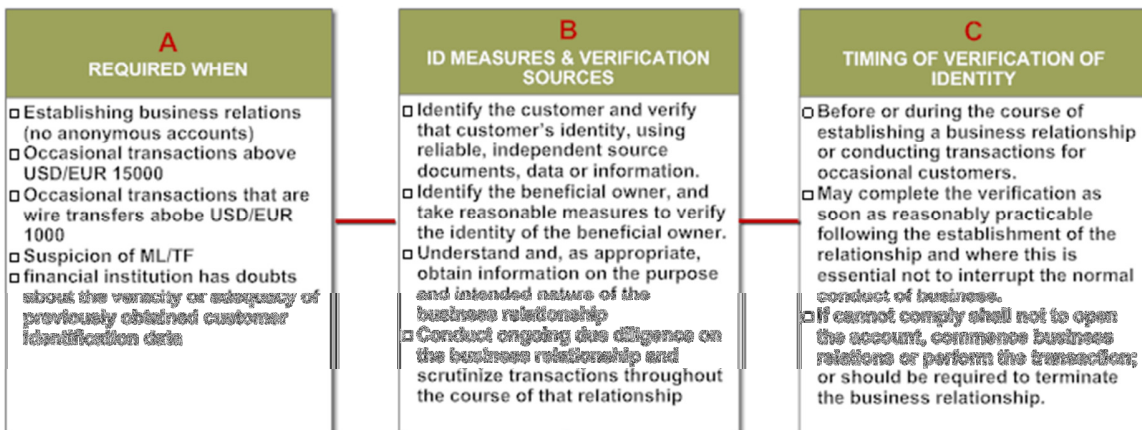
or operational function within a country) even though the basic obligation of assessing and understanding ML/TF risk rests on the country itself. The different risk assessments must relate to each other and different approaches can be advocated. For example, a top down approach means that the supranational risk assessment takes place first and informs aspects of the national assessments at country level providing a benchmark for certain judgments made in subsequent risk assessments at the country level. The second approach is a bottom up approach where the supranational assessment is informed by the results of country-level risk assessments.

3.1.3.2 FATF Recommendation 10: Customer Due Diligence

FATF Recommendation 10 requires financial institutions to perform customer due diligence (CDD) in order to identify their clients and ascertain information pertinent to doing financial business with them. “CDD requirements are intended to ensure that financial institutions can effectively identify, verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorism financing risks that they pose.”¹⁶⁸

As depicted in Diagram 3 below, Recommendation 10 contains essential components applicable to the CDD requirements for ‘standard’ customer relationships and transactions. These are 1) the description of when CDD is required, 2) identification measures and acceptable verification sources; and 3) the timing and verification of identity.

Diagram 3: Customer Due Diligence Requirements for “Standard” Customers



Whilst the CDD measures as set out in the diagram above apply to ‘standard’ customer relationships and transactions, the FATF Recommendations require the application of the risk-based approach to CDD, allowing countries to permit financial institutions to apply exemptions in low risk situations and simplified measures where there is a lower risk of money laundering and terrorist financing.¹⁶⁹

¹⁶⁸ Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 27.

¹⁶⁹ Interpretive Note to Recommendation 1, paragraph 5 and Interpretive Note to Recommendation 10, paragraphs 16 to 18 and 21.

The Interpretive Note to Recommendation 10 lists several potentially lower risk situations relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels. These are set out in Table 4 below. It is important to note that the Interpretive Note also refers to several risk variables such as the purpose of an account or relationship, the level of assets to be deposited by a customer or the size of transactions undertaken and the regularity or duration of the business relationship. These variables must be taken into account as these variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures.

In lower risk situations, such as the provision of a financial product or service that provides appropriately defined and limited services to certain types of customers so as to increase access for financial inclusion purposes (bank accounts with balance limits and restrictions on transaction values), financial service providers are permitted to apply a lighter approach to CDD. Particularly, if an account or product is for a specific purpose such as a low value account for social cash transfer recipients, the risk-based approach allows financial institutions to infer the purpose of the business relationship from the type of account established and the transactions conducted without having to verify such. These types of accounts and products may also be subject to lower levels of monitoring by financial institutions.¹⁷⁰

In most cases, some form of CDD is required but it is the “intensity and the extent of customer and transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. In a lower risk context, fulfilling CDD customer identification, verification and monitoring requirements of Recommendation 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information.”¹⁷¹

Some countries have also adopted the so called ‘progressive’ or ‘tiered’ approach to CDD. As represented in diagram 10 below, in specified circumstances such as for example for accounts or products that are subject to limited transactions, daily and monthly limits and limited account balances at any one time, financial institutions are permitted to apply simplified CDD measures at the start of the business relationship (this may be as simple as establishing the identity of the individual by accepting alternative forms of identification)¹⁷², which allow individuals to access a basic account or product without being subjected to the full CDD requirements applicable to ‘standard’ customers. Should the customer wish to undertake transactions on the account beyond the set conditions, i.e., deposit or withdraw more from the account than is allowed or wish to access additional services such as access to credit, the financial institution is required to conduct more extensive CDD measures.

As noted by FATF:

¹⁷⁰See Financial Action Task Force, *Asia/Pacific Group on Money Laundering and the World Bank Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 37 where it is noted that, “in some countries, the choice has been made to mitigate the risk introduced by simplified CDD by closely monitoring transactions linked to the relevant products and accounts. However, if little CDD is undertaken, so that the financial institution lacks a sufficient range of available information, manual or electronic scanning of transactions may not be able to deliver significant benefit”.

¹⁷¹ 30.
¹⁷² 32. It is noted that, “Using an RBA, local authorities have often allowed a broader range of documentation in pre-defined types of business relationships and for specific (financial inclusion) products and accounts, with low balance limits. Countries should take advantage of the RBA to facilitate proportionate requirements with regard to acceptable IDs that will support the provision of relevant services to unserved groups.”

“This flexible approach for limited purpose accounts, where verification is postponed but not eliminated, allows clients to get access to basic products with limited functionalities and for low value transactions. It is very useful in a financial inclusion context since it enables unbanked individuals to get access to the basic formal services they need, and at the same time reduces the costs of small value accounts and increases financial inclusion outreach for financial institutions.”¹⁷³

Two practical examples of the application of simplified CDD measures and the tiered approach to CDD are evident in the South African AML/CFT regulatory framework. South Africa’s approach to providing proven low risk exemptions and the application of simplified CDD measures in lower risk scenarios respectively, has not been to amend the Financial Intelligence Centre Act, 2001 (As Amended)¹⁷⁴ or the Money Laundering and Terrorist Financing Control Regulations, 20021 (As Amended) but instead to issue a number of separately gazetted exemptions to sections of the Financial Intelligence Centre Act, 2001 (As Amended). The most commonly referred to exemption is Exemption 17. See section J2.7.3.4.1 of Annexure J for full details on Exemption 17.¹⁷⁵

Banks Act Circular 6/2006 Cell Phone Banking was issued in 2006 by the South African Reserve Bank. Circular 6 only applies to mobile banking products, offered to clients via a non-face-to-face process, linked to a bank account covered by Exemption 17. Upon the normal interpretation of the wording of Circular 6/2006, the Circular does not apply to products that are not linked to a bank account covered by Exemption 17 despite the fact that money remitters conducting domestic transactions were included in the 2004 amendment to exemption 17. As is the case with Exemption 17, Circular 6/2006 requires observance of strict conditions (minimum criteria). See section J2.7.3.4.2 of Annexure J for further information on Circular 6/2006.¹⁷⁶

3.1.3.3 FATF Recommendation 11: Record Keeping

Recommendation 11 requires financial institutions to maintain records for at least five years of both domestic and international transactions. The records that should be maintained include all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions). These should be kept for at least five years after the termination of the business relationship or after the date of the occasional transaction. The CDD information and transactions records kept must be made available to domestic competent authorities upon appropriate authority.

Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years. A number of countries, such as the United States, Australia and Canada, have considered, but rejected, imposing photocopying obligations on their regulated institutions for a number of reasons: for example, the photocopies could be used to commit identity fraud; their retention may breach privacy laws and they may reveal information about the client that could form the basis of

¹⁷³ Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 33.

¹⁷⁴ Act 38 of 2001 (As Amended).

¹⁷⁵ Langan S and Smith K 2014 *The Legal and Regulatory Framework for Payments in 14 SADC Member States Volume II: Country Reports: South Africa Country Report* 223.

¹⁷⁶ 226.

discriminatory practices, such as the refusal of credit facilities. Recommendation 11 therefore allows for different forms of document retention, including electronic storage.

The following record retention techniques are acceptable:

- "Scanning the verification material and maintaining the information electronically;
- Keeping electronic copies of the results of any electronic verification checks;
- Merely recording (hand-writing) reference details on identity or transaction documents. This may be particularly useful in the context of mobile banking, since mobile money agents are often basic corner shops. The types of details it is advisable to record include:
 - Reference numbers on documents or letters,
 - Relevant dates, such as issue, expiry or writing,
 - Details of the issuer or writer,
 - All identity details recorded on the document."¹⁷⁷

3.1.2.4 FATF Recommendation 13: Correspondent Banking

FATF Recommendation 13 requires financial institutions when engaging in cross-border correspondent banking and other similar relationships, in addition to performing normal CDD measures to gather sufficient information about the respondent institution, assess the respondent institution's AML/CFT controls and obtain senior management approval when establishing a new correspondent relationship. Sending banks and receiving banks must also clearly understand the respective responsibilities of each institution. With respect to payable through accounts, the sending bank must be satisfied that the receiving bank has conducted CDD on the customers having direct access to accounts of the correspondent bank and that the respondent bank is able to provide relevant information upon request. The Recommendation further requires that financial institutions should be prohibited from entering into or continuing a correspondent relationship with shell banks.

Correspondent banking is relevant to the financial inclusion debate as when alternative cross-border remittance channels such as Western Union MoneyGram are not available, individuals are required to rely on their banks correspondent banking relationships in order to effect cross-border payments. Whilst most individuals sending or receiving cross-border payments have no idea about the behind the scenes workings of a typical correspondent banking model, this Recommendation is vital as it structures the manner in which correspondent relationships should be set up.

3.1.3.5 FATF Recommendation 14: Money or Value Transfer Services

FATF Recommendation 14 requires countries to take measures to ensure that natural and legal persons that provide money or value transfer services (MVTs) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the measures set out in the FATF Recommendations. Of particular relevance to the financial inclusion agenda is the requirement set out in Recommendation 14 that "any natural or legal person working as an agent should be licensed or registered by a competent authority, or the Money Value Transfer Service (MVTs) provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTs provider and its agents operate." It is important to note that this

¹⁷⁷ Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 39.

requirement on agents only exists in the context of money and value transfer services – and not for other types of financial services covered by the FATF Recommendations.

3.1.3.6 FATF Recommendation 15: New Technologies

Recommendation 15 introduces new technologies that may require enhanced CDD measures. This recommendation requires countries and financial institutions to identify and assess the money laundering or terrorist financing risks that may arise in relation to the development of new products, new business practices and delivery mechanisms. In addition, the recommendation requires financial institutions to undertake a risk assessment prior to the launch of a new product, the introduction of a new business practice or the use of new or developing technologies. Appropriate measures must be taken to manage and mitigate risks. Innovations in the payments space, including new channels of delivery such as the internet and mobile banking, online credit card payments and advances in products (prepaid cards, hybrid cards mobile money transfer etc.) mean that many transactions are conducted in a non-face-to-face environment. Whilst FATF has not released an Interpretive Note for Recommendation 15, it has released a guidance paper on prepaid cards, mobile payments and Internet-based payment services.¹⁷⁸ The paper refers to these innovative payment products and services as “new payment products and services” (NPPS).¹⁷⁹ The paper proposes guidance on the risk-based approach to AML/CFT measures and regulation in relation to NPPS of prepaid cards, mobile payments and Internet-based payment services, in line with the FATF Recommendations.

3.1.3.7 FATF Recommendation 16: Wire Transfers

Recommendation 16 applies to cross-border wire transfers and domestic wire transfers, including serial payments, and cover payments.¹⁸⁰ Recommendation 16 does not however cover transfers that flow from a transaction carried out using a credit or debit card for the purchase of goods or services, as long as the payment card number accompanies all transfers flowing from the transaction¹⁸¹ and financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf. For cross-border wire transfers, the information accompanying all qualifying wire transfers should always contain:

- (a) The name of the originator;
- (b) The originator account number where such an account is used to process the transaction;
- (c) The originator’s address, or national identity number, or customer identification number, or date and place of birth;
- (d) The name of the beneficiary; and
- (e) The beneficiary account number where such an account is used to process the transaction.¹⁸²

¹⁷⁸ See Financial Action Task Force (FATF) *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services 4* where the following is stated, “For the purposes of this guidance, NPPS are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations.”

¹⁷⁹

¹⁸⁰ Interpretative Note 16, paragraph 3.

¹⁸¹ However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

¹⁸² Interpretative Note to Recommendation 16, paragraph 6.

In the absence of an account, a unique transaction reference number should be included which will allow for transaction traceability. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from [these] requirements in respect of originator information, provided that they include the originator's account number or unique transaction reference number, [...] and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.¹⁸³

In the case of domestic wire transfers, the accompanying information should include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. As wire transfers are often used as a remittance channel where no other cheaper and more convenient options exist, the *de minimis* threshold of USD1,000 is of particular relevance.¹⁸⁴

Interpretive Note 16 paragraph 5 states:

"Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

- (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
- (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information."

It is important to note that financial institutions are still required to include the name of the originator; the name of the beneficiary; and an account number for each, or a unique transaction reference number with the cross-border wire transfer, but are not required to verify this information.

3.1.3.8 FATF Recommendation 17: Reliance on Third Parties

Countries may permit financial institutions to rely on third parties to perform several of the CDD measures set out in Recommendation 10 or to introduce business. However, financial institutions relying on third parties must ensure that copies of identification data and other relevant documentation relating to CDD requirements will be made available to the financial institution from the third party upon request and without delay. Financial institutions must also satisfy themselves that the third party is regulated, supervised or monitored, and has

¹⁸³ Paragraph 7.

¹⁸⁴ See Langan S and Kilfoil K 2011 *The Cross-border Money Transfer Experience Why Taxes and Buses are Still Preferred to Banks*.

measures in place to meet the CDD and record keeping requirements set out in Recommendations 10 and 11.¹⁸⁵ For the purposes of financial inclusion, new technologies and branchless banking, the ability to rely on third parties to secure the customer is vital to the sustainability of the business model, the customer experience and the circumstances of low income customers.

It is important to note that recommendation 17 does **not** apply to outsourcing or agency relationships. The third party, defined in Interpretive Note 17, paragraph 3 as “financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17,” will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the third party, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with prescribed procedures, and is subject to the delegating financial institution’s control of the effective implementation of these procedures, by the outsourced entity.

3.1.3.9: FATF Recommendation 20: Suspicious Transaction Reporting

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit. Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. As this is a mandatory requirement, applying the risk-based approach to the requirements to report suspicious transactions is a moot point.

However, as noted by FATF in the 2013 Financial Inclusion guidance:

“The [risk-based approach] RBA is, however, appropriate for the purpose of identifying potentially suspicious activity, for example, by directing additional resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk. As part of an RBA, it is also likely that a financial institution will utilize information (typologies, alerts, guidance) provided by competent authorities to inform its approach for identifying suspicious activity. A financial institution should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions. FATF Recommendation 20 stipulates that if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, it should be required to report the incident promptly to the country’s Financial Intelligence Unit (FIU). This obligation applies to all financial institutions that are subject to AML/CFT obligations, including those that serve disadvantaged and low income people. The implementation of such a requirement requires financial institutions to put in place appropriate internal monitoring systems to identify any unusual behavior.”¹⁸⁶

¹⁸⁵ Recommendation 17 states further that, “When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.”

¹⁸⁶ Financial Action Task Force, *Asia/Pacific Group on Money Laundering and the World Bank Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion 40*.

3.1.3.10: FATF Recommendation 34: Guidance and Feedback

Recommendation 34 covering guidance and feedback is not covered in the 2013 FATF Financial Inclusion paper. As the primary purpose of this report is to set out the legal and regulatory framework for AML/CFT in various SADC countries and to propose measures which could lead to a harmonised approach with particular emphasis being placed in financial inclusion, we highlight Recommendation 34 as being a vital recommendation needed in order to support the financial inclusion agenda.

Recommendation 34 states that, the competent authorities, supervisors and [Supervisory and Regulatory Bodies] (SRBs) should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

Several of the individuals and organisations, including Commercial Banks, who were interviewed during the course of this research, highlighted the lack of guidance notes and feedback from the FIU as a considerable area of frustration. Proposals included in Part C of this report cover the need for Regulators and the FIU in each country to establish guidelines (particularly with respect to the application of the risk-based approach) and to provide financial institutions, designated Non-bank Financial Institutions (NBFIs) and Designated Non-Financial Businesses and Professions (DNFBPs) with feedback on the appropriateness and usefulness of suspicious transaction reports submitted by them. Section B of the report highlights the fact that several laws and regulations do not include provisions mandating the issuing of guidelines and feedback.

3.1.4 The BIS/World Bank General Principles for International Remittance Services

In 2007, the World Bank and the Bank of International Settlements published the *General Principles for International Remittance Services* report.¹⁸⁷ The purpose of the report is to analyse the payment system aspects of remittances and provide general principles to assist countries that want to improve the market for remittance transfers. As noted in the report, “the principles are not intended to be prescriptive but rather to give guidance. The application of the principles should help to achieve the public policy objectives of having safe and efficient international remittance services, which require the markets for the services to be contestable, transparent, accessible and sound.” The five principles set out in the report are summarised in Table 12 below.

Table 12: Five Principles for International Remittance Services

Ref	Principle
Principle 1	Transparency and consumer protection The market for remittance services should be transparent and have adequate consumer protection.
Principle 2	Payment system infrastructure Improvements to payment system infrastructure that have the potential to increase the efficiency of remittance services should be encouraged.
Principle 3	Legal and regulatory environment Remittance services should be supported by a sound, predictable, nondiscriminatory and proportionate legal and regulatory framework in relevant jurisdictions.

¹⁸⁷ World Bank and Bank for International Settlements 2007 *General Principles for International Remittance Services*.

Principle 4	Market structure and competition Competitive market conditions, including appropriate access to domestic payment infrastructures, should be fostered in the remittance industry.
Principle 5	Governance and risk management Remittance services should be supported by appropriate governance and risk management practices.

For the purposes of this report, Principle 1 and Principle 3 are particularly relevant. Principle 1 requires the market for remittances to be transparent and have adequate consumer protection. This means that the price to the remitter should be transparent. Pricing depends on: 1) the exchange rate used and 2) fees charged. Combining the two to calculate the cost of the service is often difficult and often not transparent to the remitter. Remittance Service Providers should be encouraged to provide relevant information about their services in accessible and understandable forms and comparative price information should be given. This requirement may be included in the Consumer Protection Act or a fit for purpose Regulation or Directive such as the Angolan Aviso No. 06/12 of 29 March that regulates the provision of remittances services.

Principle 3 requires that Remittance Services be supported by a sound, predictable, non-discriminatory and proportionate legal and regulatory framework in relevant jurisdictions. There is a possibility that laws and regulations that are badly designed have unintended consequences, which are disproportionate to the problem that the laws and regulations were designed to address. Regulating remittances by type of entity (licensed institutions) may make regulation less effective and distort markets. National regulations are encouraged to aim to create a level playing field between equivalent remittance services and not favour one type over another. Directive 2007/64/EC Payment Services in the Internal Market (PSD) which was adopted by the European Parliament and the Council in November 2007 is an example of hard law designed to create a harmonised legal framework for payments, including remittance payments. As noted by the European Central Bank, "the Directive aims to create a harmonised legal framework for payments (seeking in particular to establish a legal basis for SEPA), thereby ensuring that cross-border payments within the European Union (particularly credit transfers, direct debits and card payments) can be carried out just as easily, efficiently and securely as domestic payments within the various Member States. It also establishes the concept of "payment institutions" – licensed payment service providers that are able to provide payment services across the European Union under lighter supervisory regime than banks. By opening up the market in this way, the European legislator is seeking to allow new service providers to compete with existing participants on a level playing field, thereby facilitating greater competition."

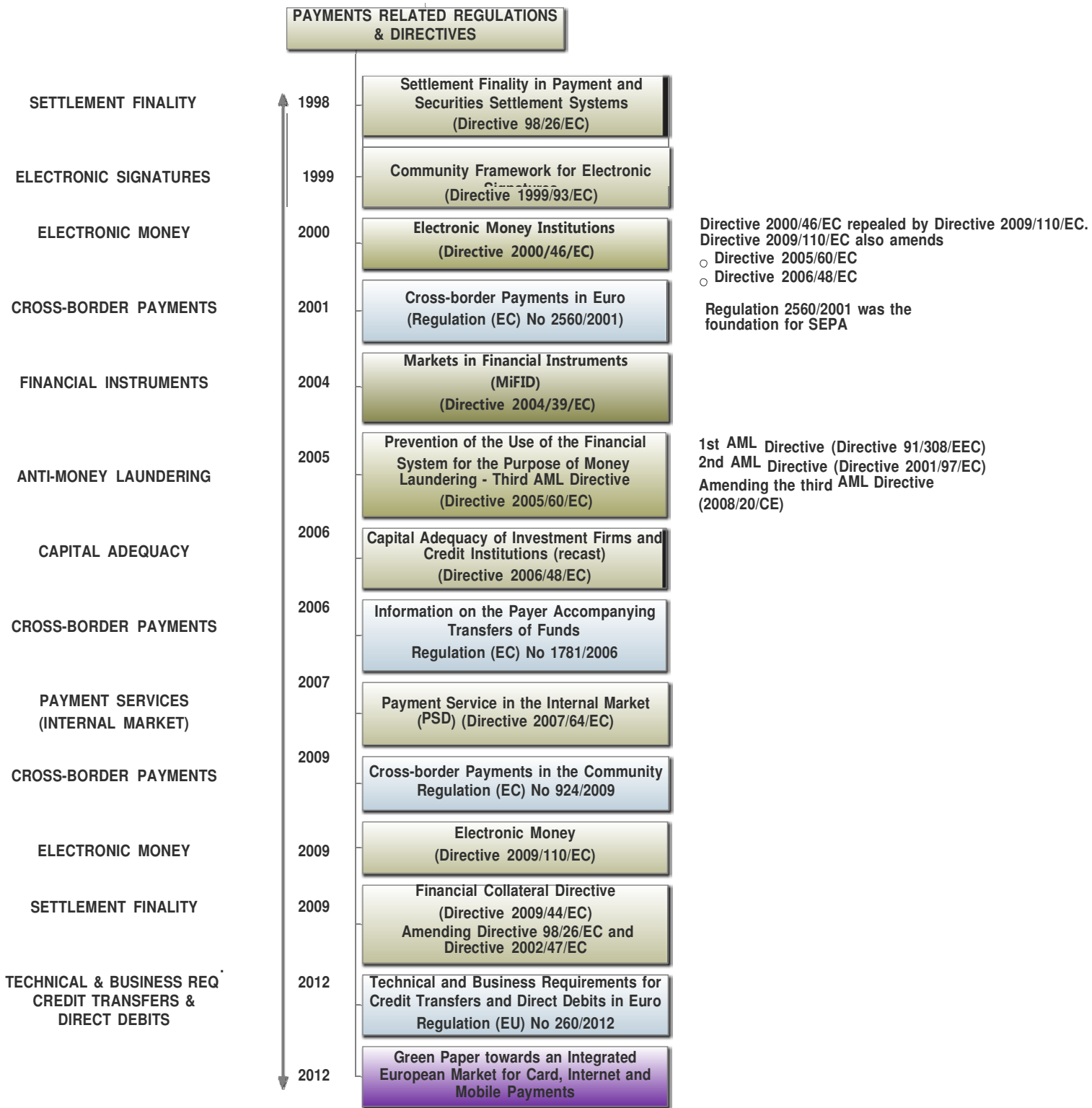
3.2 European Union Regulations and Directives (Hard Law)

As noted in the introduction above, the SIRESS project is patterned explicitly after the SEPA. Consequently, the regulatory framework adopted by the EU serves as an appropriate benchmark when considering the harmonisation of payment, clearing and settlement system laws and regulations in the SADC region. In the section that follows, the provisions included in the three primary EU Regulations adopted together with best practice principles drawn from several Directives are discussed. In addition, as directives must be transposed into domestic law or regulation, several examples of the approach taken by Member States in this regard are set out in detail.

Diagram 4 below shows the evolution of the common regulatory framework for payments in the EU, from the humble beginnings, where the Community legislator's response to the concerns identified by the Committee on Payment and Securities Systems (CPSS) under the auspices of the Bank for International Settlements

regarding systemic risk resulted in Directive 98/26/EC being adopted to the latest Green Paper, *Towards an Integrated European Market for Card, Internet and Mobile Payments* that was published in November 2012.

Diagram 4: European Union – Evolution of a Common Regulatory Framework for Payments



3.2.1 The EC Regulations

Regulations are binding in their entirety and directly applicable to all Member States. "Regulations are adopted by the Council or by the Council together with the Parliament through the so-called 'co-decision' procedure, by the Commission and by the European Central Bank."¹⁸⁸ An additional feature of this form of community law is that regulations are directly applicable to all Member States, meaning that national measures such as ratification are not required before the regulation is binding on Member States, institutions, undertakings and natural persons. Community law always has precedence over national law.

The first payments related Regulation adopted was Regulation (EC) No 2560/2001 on Cross-border Payments in Euro that was adopted in 2001. As noted by the European Payments Council, "the Commission laid the foundations of its Single Euro Payments Area (SEPA) policy through former Regulation 2560/2001 on cross-border payments in euro, whereby banks are not permitted to impose different charges for domestic and cross-border payments or ATM withdrawals in the EU-27. Regulation 2560/2001 has also generally been understood as a turning point in the financial integration policy of the European legislator: beyond its formal stipulations, the Regulation at the time of its inception was clearly intended to shock the banking sector into stepping up its efforts to achieve the Single Euro Payments Area (SEPA)."¹⁸⁹ The revised version of this Regulation, Regulation (EC) No 924/2009 on Cross-border Payments in the Community was approved by the European Parliament on 24 April 2009.

The second, Regulation (EC) No 1781/2006 on Information on the Payer Accompanying Transfers of Funds, lays down rules for payment service providers to send information on the payer throughout the payment chain. This is done for the purposes of prevention, investigation and detection of money laundering and terrorist financing.¹⁹⁰ In December 2010 the European Commission published a proposal for a regulation establishing EU-wide requirements for credit transfers and direct debits in euro. The final regulation, Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro came into effect on 31 March 2012 after its adoption by the EU Council and the European Parliament in February 2012. Regulation No 260/2012 sets 1 February 2014 as the deadline in the euro area for replacing national credit transfers and direct debits with their SEPA equivalents. In Member States with other currencies, the deadline is 31 October 2016. The regulation also requires the use of certain common standards and technical requirements, such as the use of International Bank Account Numbers (IBAN), Business Identifier Codes (BIC) and the financial services messaging standard ISO 20022 XML for all credit transfers and direct debits in euro in the EU. In the section below, the provisions included in each Regulation are discussed in depth.

¹⁸⁸ See Mathijssen P A *Guide to European Union Law* (2004).

¹⁸⁹ See European Payments Council (EPC) AISBL 2009 *Making SEPA a Reality - The definitive Guide to the Single Euro Payments Area*. Available at: http://www.sepaesp.es/f/websepa/secciones/Sobre/18-folleto_epc_0901.pdf where it is noted further that, "the revised version of this Regulation approved by the European Parliament on 24 April 2009 introduces additional provisions which - in the eyes of the regulator - further promote EU financial integration in general and SEPA implementation in particular. The revised Regulation has significant impact due to the introduction of the following provisions: (1) the price parity requirements are extended to direct debits; (2) the setting out of clear rules for transaction-based multilateral interchange fees until November 2012; (3) banks in the euro area offering direct debits today in euro to debtors are mandated to become reachable for SEPA Direct Debit collections from November 2010 onwards. The revised Regulation - now labelled Regulation on cross-border payments in euro in the Community - will be applicable in all Member States from 1 November 2009 onwards."

¹⁹⁰ The Regulation transposes Special Recommendation VII (SRVII) of the Financial Action Task Force (FATF) into EU law and is part of the EU Plan of Action to Combat Terrorism. Special Recommendation VII (SRVII) has been renumbered as Recommendation 16 in the Financial Action Task Force (FATF) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*.

3.2.1.1 Regulation (EC) No 924/2009 Cross-border Payments in the Community

The first Regulation on cross-border payments in Euro, Regulation (EC) No 2560/2001 was passed in 2001. This Regulation was subsequently repealed by Regulation (EC) No 924/2009. The text that follows provides a summary of the most important regulations contained in Regulation (EC) No 924/2009.

Recital: Equality of charges for cross-border payments: Recital 1 confirms that for the proper functioning of the internal market and in order to facilitate cross-border trade within the Community it is essential that the charges for cross-border payments in euro are the same as for corresponding payments within a Member State.¹⁹¹

Recital: Common Business Model and Legal Certainty on Multilateral Interchange Fees: Recital 11 states that, “currently, different business models are used for existing national direct debit schemes. To facilitate the launch of the SEPA direct debit scheme, it is necessary to put in place a common business model and provide greater legal clarity on multilateral interchange fees. For cross-border direct debits, this could be achieved, exceptionally, by establishing a maximum amount for the multilateral interchange fee per transaction during a transitional period. The parties to a multilateral agreement should, however, be free to determine a lower amount or agree a zero multilateral interchange fee. For national SEPA direct debits, the same national interchange fee or other agreed inter-bank remuneration between the payment service providers of the payee and of the payer could be used as that which existed before the date of application of this Regulation.” The Recital states further that, “where the direct debit transaction is subject to a bilateral agreement, however, the terms of such a bilateral agreement should take precedence over any multilateral interchange fee or other agreed interbank remuneration. Industry can make use of the legal certainty provided during the transitional period to develop and agree a common, long-term business model for the operation of the SEPA direct debit. At the end of the transitional period, a long-term solution for the SEPA direct debit business model should be in place in line with EC competition law and the Community regulatory framework.”

Recital: Reachability of Payer’s Account: Recital 12 notes that, “for a direct debit transaction to be executed, the payer’s account must be reachable.¹⁹² To encourage the successful take-up of SEPA direct debits, it is therefore vital that all payer accounts be reachable where this is already the case for existing national direct debits denominated in euro, otherwise the payer and the payee will be unable to enjoy the benefits of cross-border direct debit collection. If the payer account is not reachable under the SEPA direct debit scheme, the payer (debtor) and the payee (creditor) will be unable to benefit from the new direct debit payment opportunities available. This is especially important where the payee initiates direct debit collections in a batch file, for example on a monthly or quarterly basis for electricity or other utility bills, and not as a separate collection for each customer. .” A one year grace period is afforded to payment service providers following the date of application of this Regulation in order to comply with the reachability obligation.

Recital: Complaints Redress: In order to ensure that redress is possible where the Regulation has been incorrectly applied, Member States are required to establish adequate and effective complaint and redress procedures for settling any dispute between the payment service user and the payment service provider

¹⁹¹ The principle of equality of charges is established by Regulation (EC) No 2560/2001 of the European Parliament and of the Council of 19 December 2001 on cross-border payments in euro, which applies to cross-border payments in euro and in Swedish kronor up to EUR 50 000, or equivalent.

¹⁹² The reachability obligation encompasses the right of a payment service provider not to execute a direct debit transaction in accordance with the direct debit scheme regarding, for example, the rejection, refusal or return of transactions. The reachability obligation should, furthermore, not apply to payment service providers which have been authorised to provide and execute direct debit transactions but which do not engage commercially in such activities.

(Recital 15). The Recital states further that it is important that competent authorities and out-of court complaint and redress bodies are appointed either by designating existing bodies, where appropriate, or by establishing new bodies. Competent authorities and out-of-court complaint and redress bodies, within the Community are required to actively cooperate for the smooth and timely resolution of cross-border disputes under the Regulation.

Scope: Regulation (EC) No 924/2009 lays down rules on cross-border payments¹⁹³ within the Community and ensures that charges for cross-border payments within the Community are the same as those for payments in the same currency within a Member State.¹⁹⁴ The Regulation does not apply to payments made by payment service providers for their own account or on behalf of other payment service providers.¹⁹⁵

Charges for Cross-border Payments and Corresponding National Payments: Article 3 specifically requires that charges levied by a payment service provider on a payment service user in respect of cross-border payments of up to EUR 50 000 must be the same as the charges levied by that payment service provider on payment service users for corresponding national payments of the same value and in the same currency. The Regulation does not however apply to currency conversion charges.¹⁹⁶

Measures for Facilitating the Automation of Payments: Article 4 covers measures for facilitating the automation of payments and requires payment service providers where applicable, to communicate to the payment service user the payment service user's International Bank Account Number (IBAN) and the payment service provider's Business Identifier Code (BIC).¹⁹⁷ In addition, where applicable, a payment service provider must indicate the payment service user's IBAN and the payment service provider's BIC on statements of account, or in an annex thereto.¹⁹⁸

Balance of Payments Reporting Obligations: Article 5(1) provides that, "with effect from 1 January 2010, Member States shall remove settlement-based national reporting obligations on payment service providers for balance of payments statistics related to payment transactions of their customers up to EUR 50 000."

Interchange Fee for Cross-border Direct Debit Transactions: As per Article 6, in the absence of any bilateral agreement between the payment service providers of the payee and of the payer) sets the multilateral interchange fee to EUR 0,088, payable by the payment service provider of the payee to the payment service provider of the payer. This applies for each cross-border direct debit transaction executed before 1 November 2012, unless a lower multilateral interchange fee is agreed upon between the payment service providers concerned.

Reachability for direct debit transactions: Article 8 deals with the reachability of direct debit transactions and requires that a payment service provider of a payer reachable for a national direct debit transaction denominated in euro on the payment account of that payer is reachable, in accordance with the direct debit scheme, for direct debit transactions denominated in euro initiated by a payee through a payment service

¹⁹³ Article 2(1) of Regulation (EC) No 924/2009 defines a cross-border payment as, "an electronically processed payment transaction initiated by a payer or by or through a payee where the payer's payment service provider and the payee's payment service provider are located in different Member States."

¹⁹⁴ Article 1(1) of Regulation (EC) No 924/2009.

¹⁹⁵ Article 1(3).

¹⁹⁶ Article 3(4).

¹⁹⁷ Article 4(1).

¹⁹⁸ This information must be provided free of charge.

provider located in any Member State. This applies only to direct debit transactions which are available to consumers under the direct debit scheme.

Competent authorities: Article 9 requires Member States to designate the competent authorities responsible for ensuring compliance with the Regulation. Member States were required to notify the Commission of those competent authorities by 29 April 2010.

Complaint procedures for alleged infringements of the Regulation: Member States are required to establish procedures which allow payment service users and other interested parties to submit complaints to the competent authorities with regard to alleged infringements of this Regulation by payment service providers.

Out-of-court complaint and redress procedures: Member States are required in compliance with Article 11 to establish adequate and effective out-of-court complaint and redress procedures for the settlement of disputes concerning rights and obligations arising under the Regulation between payment service users and their payment service providers. For those purposes, Member States may designate existing bodies, or, where appropriate, establish new bodies.

Cross-border cooperation: Article 12 requires the competent authorities and the bodies responsible for out-of-court complaint and redresses procedures of the different Member States to actively and expeditiously cooperate in solving cross-border disputes.

Penalties: In terms of Article 13, Member States were given until the 1 June 2010 to lay down rules on the penalties applicable to infringements to the Regulation and to take all measures necessary to ensure that they are implemented. Such penalties are required to be effective, proportionate and dissuasive.

3.2.1.2 Regulation EC No 178/2006 Information on the Payer Accompanying Transfers of Funds

Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds lays down rules for payment service providers to send information on the payer throughout the payment chain. This is done for the purposes of prevention, investigation and detection of money laundering and terrorist financing.¹⁹⁹

Scope of Application: Article 3 sets out the scope of application of the Regulation. The Regulation applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the Community. It does not apply to transfers of funds carried out using a credit or debit card, provided that the payee has an agreement with the payment service provider permitting payment for the provision of goods and Services and a unique identifier, allowing the transaction to be traced back to the payer, accompany such transfer of funds.

Article 3(3) states that where a Member State chooses to apply the derogation set out in **Article 11(5)(d) of Directive 2005/60/EC**, that Regulation 924/2009 does not apply to transfers of funds using electronic money covered by that derogation, except where the amount transferred exceeds EUR 1 000. Further, as per Article 3(4), the regulation does not apply to transfers of funds carried out by means of a mobile telephone or any other digital or Information Technology (IT) device, when such transfers are pre-paid and do not exceed EUR150. This Regulation does not apply to transfers of funds carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions: (a) the

¹⁹⁹ The Regulation transposes the old Special Recommendation VII (SRVII) of the Financial Action Task Force (FATF) into EU law and is part of the EU Plan of Action to Combat Terrorism.

payee has an agreement with the payment service provider permitting payment for the provision of goods and services; (b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds; and (c) the payment service provider is subject to the obligations set out in Directive 2005/60/EC.

Member States are at liberty in terms of Article 3(6) to decide not to apply the Regulation to transfers of funds within that Member State to a payee account permitting payment for the provision of goods or services if: (a) the payment service provider of the payee is subject to the obligations set out in Directive 2005/60/EC; (b) the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services; and (c) the amount transacted is EUR 1 000 or less.

The Regulation is also not applicable to transfers of funds where (a) the payer withdraws cash from his or her own account; (b) where there is a debit transfer authorisation between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds, enabling the natural or legal person to be traced back; (c) where truncated cheques are used; (d) to public authorities for taxes, fines or other levies within a Member State; and (e) where both the payer and the payee are payment service providers acting on their own behalf (Article 3(7)).

Complete information on the payer: Article 4 defines what “complete information on the payer” consists of and is set out as follows: name, address and account number. The address may be substituted with the date and place of birth of the payer, his customer identification number or national identity number. In the case where the payer does not have an account number, the payment service provider of the payer is required to substitute it by a unique identifier that allows the transaction to be traced back to the payer.

Information accompanying transfers of funds and record keeping: In terms of Article 5, payment service providers are required to ensure that transfers of funds are accompanied by complete information on the payer. Before transferring the funds, the payment service provider of the payer is required to verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source. In the case of transfers of funds from an account, verification is deemed to have taken place if: (a) a payer’s identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in Articles 8(2) and 30(a) of Directive 2005/60/EC; or the payer falls within the scope of Article 9(6) of Directive 2005/60/EC. However, without prejudice to Article 7(c) of Directive 2005/60/EC, in the case of transfers of funds not made from an account, the payment service provider of the payer is required to verify the information on the payer only where the amount exceeds EUR 1 000, unless the transaction is carried out in several operations that appear to be linked and together exceed EUR 1 000. Payment service providers of the payer are required to keep records of complete information on the payer which accompanies transfers of funds for a period of five years.

Transfers of funds within the Community: Article 6 provides derogation from article 5 where both the payment service provider of the payer and the payment service provider of the payee are situated in the Community. In this case, transfers of funds are required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer. However, if so requested by the payment service provider of the payee, the payment service provider of the payer is required to make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

Transfers of funds from the Community to outside the Community: The transfers of funds where the payment service provider of the payee is situated outside the Community must be accompanied by complete information on the payer (Article 7(1)).²⁰⁰

3.2.1.3 Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro

The most recent EU Regulation, Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro lays down rules for credit transfer and direct debit transactions denominated in euro within the Union where both the payer's payment service provider and the payee's payment service provider are located in the Union, or where the sole payment service provider (PSP) involved in the payment transaction is located in the Union.²⁰¹ The Regulation does not apply to:

- payment transactions carried out between and within PSPs, including their agents or branches, for their own account;
- payment transactions processed and settled through large-value payment systems, excluding direct debit payment transactions which the payer has not explicitly requested be routed via a large-value payment system;
- payment transactions through a payment card or similar device, including cash withdrawals, unless the payment card or similar device is used only to generate the information required to directly make a credit transfer or direct debit to and from a payment account identified by Base Bank Account Number (BBAN) or IBAN;
- payment transactions by means of any telecommunication, digital or IT device, if such payment transactions do not result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN;
- transactions of money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC;
- payment transactions transferring electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC unless such transactions result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN.

Key definitions:

Credit transfer means a national or cross-border payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer.

Direct debit means a national or cross-border payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent.

Payer means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payer's payment account, a natural or legal person who makes a payment order to a payee's payment account.

²⁰⁰ As per Article 7(2), "in the case of batch file transfers from a single payer where the payment service providers of the payees are situated outside the Community, paragraph 1 shall not apply to the individual transfers bundled together therein, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier."

²⁰¹ Article 1(1) of Regulation (EU) No 260/2012.

Payee means a natural or legal person who holds a payment account and who is the intended recipient of funds which have been the subject of a payment transaction.

Reachability: Article 3(1) requires a payee's PSP which is reachable for a national credit transfer under a payment scheme to be reachable, in accordance with the rules of a Union-wide payment scheme, for credit transfers initiated by a payer through a PSP located in any Member State and Article 3(2) requires a payer's PSP which is reachable for a national direct debit under a payment scheme to be reachable, in accordance with the rules of a Union-wide payment scheme, for direct debits initiated by a payee through a PSP located in any Member State.

Interoperability: In terms of Article 4(1), payment schemes to be used by PSPs for the purposes of carrying out credit transfers and direct debits are required to comply with a number of conditions. These are as follows:

- rules are the same for national and cross-border credit transfer transactions within the Union and similarly for national and cross-border direct debit transactions within the Union; and
- the participants in the payment scheme represent a majority of PSPs within a majority of Member States, and constitute a majority of PSPs within the Union, taking into account only PSPs that provide credit transfers or direct debits respectively.

Article 4(2) requires the operator or, in the absence of a formal operator, the participants of a retail payment system within the Union to ensure that their payment system is **technically interoperable** with other retail payment systems within the Union through the use of standards developed by international or European standardisation bodies. In addition, they may not adopt business rules that restrict interoperability with other retail payment systems within the Union. Payment systems designated under Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems are only obliged to ensure technical interoperability with other payment systems designated under the same Directive.

Requirements for Credit Transfer and Direct Debit Transactions: PSPs are required to carry out credit transfer and direct debit transactions in accordance requirements set out in Article 5 of the Regulation. These requirements are summarised as follows:

- PSPs must use the payment account identifier specified in point (1)(a) of the Annex for the identification of payment accounts regardless of the location of the PSPs concerned (Article 5(1)(a));²⁰²
- PSPs must use the message formats specified in point (1)(b) of the Annex, when transmitting payment transactions to another PSP or via a retail payment system (Article 5(1)(b));²⁰³
- PSPs must ensure that payment service users (PSUs) use the payment account identifier specified in point (1)(a) of the Annex for the identification of payment accounts, whether the payer's PSP and the payee's PSP or the sole PSP in the payment transaction are located in the same Member State or in different Member States (Article 5(1)(c));²⁰⁴

²⁰² The payment account identifier referred to in Article 5(1)(a) and (c) must be IBAN.

²⁰³ The standard for message format referred to in Article 5(1)(b) and (d) must be the ISO 20022 XML standard.

²⁰⁴ The payment account identifier referred to in Article 5(1)(a) and (c) must be IBAN.

- PSPs must ensure that where a payment service user (PSU) that is not a consumer or a microenterprise, initiates or receives individual credit transfers or individual direct debits which are not transmitted individually, but are bundled together for transmission, the message formats specified in point (1)(b) of the Annex are used (Article 5(1)(d));²⁰⁵

In terms of Article 5(2), PSPs are required to carry out **credit transfers** in accordance with the following requirements, subject to any obligation laid down in the national law implementing Directive 95/46/EC:²⁰⁶

- the payer's PSP must ensure that the payer provides the data elements specified in point (2)(a) of the Annex (Article 5(2)(a));²⁰⁷
- the payer's PSP must provide the data elements specified in point (2)(b) of the Annex to the payee's PSP (Article 5(2)(b));²⁰⁸
- the payee's PSP must provide or make available to the payee the data elements specified in point (2)(d) of the Annex (Article 5(2)(c)).²⁰⁹

In terms of Article 5(3), PSPs are required to carry out **direct debits** in accordance with the following requirements, subject to any obligation laid down in national law implementing Directive 95/46/EC:

- the payee's PSP must ensure that the payee provides the data elements specified in point (3)(a) of the Annex with the first direct debit and one-off direct debit and with each subsequent payment transaction (Article 5(3)(a)(i));²¹⁰
- the payee's PSP must ensure that: the payer gives consent both to the payee and to the payer's PSP (directly or indirectly via the payee), the mandates, together with later modifications or cancellation, are stored by the payee or by a third party on behalf of the payee and the payee is informed of this obligation by the PSP in accordance with Articles 41 and 42 of Directive 2007/64/EC (Article 5(3)(a)(ii));
- the payee's PSP must provide the payer's PSP with the data elements specified in point (3)(b) of the Annex (Article 5(3)(b));²¹¹

²⁰⁵ The standard for message format referred to in Article 5(1)(b) and (d) must be the ISO 20022 XML standard.

²⁰⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data

²⁰⁷ The data elements referred to in Article 5(2)(a) are the following: (i) the payer's name and/or the IBAN of the payer's payment account, (ii) the amount of the credit transfer, (iii) the IBAN of the payee's payment account, (iv) where available, the payee's name, (v) any remittance information.

²⁰⁸ The data elements referred to in Article 5(2)(b) are the following: (i) the payer's name, (ii) the IBAN of the payer's payment account, (iii) the amount of the credit transfer, (iv) the IBAN of the payee's payment account, (v) any remittance information, (vi) any payee identification code, (vii) the name of any payee reference party, (viii) any purpose of the credit transfer, (ix) any category of the purpose of the credit transfer.

²⁰⁹ The data elements referred to in Article 5(2)(c) are the following: (i) the payer's name, (ii) the amount of the credit transfer, (iii) any remittance information.

²¹⁰ The data elements referred to in Article 5(3)(a)(i) are the following: (i) the type of direct debit (recurrent, one-off, first, last or reversal), (ii) the payee's name, (iii) the IBAN of the payee's payment account to be credited for the collection, (iv) where available, the payer's name, (v) the IBAN of the payer's payment account to be debited for the collection, (vi) the unique mandate reference, (vii) where the payer's mandate is given after 31 March 2012, the date on which it was signed, (viii) the amount of the collection, (ix) where the mandate has been taken over by a payee other than the payee who issued the mandate, the unique mandate reference as given by the original payee who issued the mandate, (x) the payee's identifier, (xi) where the mandate has been taken over by a payee other than the payee who issued the mandate, the identifier of the original payee who issued the mandate, (xii) any remittance information from the payee to the payer, (xiii) any purpose of the collection, (xiv) any category of the purpose of the collection.

- the payee's PSP must provide or make available to the payee the data elements specified in point (2)(d) of the Annex (Article 5(3)(c));²¹²
- the payer must have the right to instruct its PSP to limit a direct debit collection to a certain amount or periodicity or both (Article 3(d)(i));
- the payer must have the right to instruct its PSP, where a mandate under a payment scheme does not provide for the right to a refund, to verify each direct debit transaction, and to check whether the amount and periodicity of the submitted direct debit transaction is equal to the amount and periodicity agreed in the mandate, before debiting their payment account, based on the mandate-related information (Article 3(d)(ii)); ;
- the payer must have the right to instruct its PSP to block any direct debits to the payer's payment account or to block any direct debits initiated by one or more specified payees or to authorise direct debits only initiated by one or more specified payees (Article 3(d)(iii)).

Upon the first direct debit transaction or a one-off direct debit transaction and upon each subsequent direct debit transaction, the payee is required to send the mandate-related information to his or her PSP and the payee's PSP is required to transmit that mandate-related information to the payer's PSP with each direct debit transaction.²¹³

End Dates: Article 6 of the Regulation sets several end dates for compliance with the technical standards set out in the Regulation. This (subject to Article 6(3)) is set as the 1 February 2014 for both credit transfers and direct debits.

Validity of mandates and right to a refund: As per Article 7, valid payee authorisations to collect recurring direct debits in a legacy schemes prior to 1 February 2014 continue to remain valid after that date and are considered as representing the consent to the payer's PSP to execute the recurring direct debits collected by that payee in compliance with the Regulation in the absence of national law or customer agreements continuing the validity of direct debit mandates.

Interchange fees for direct debit transactions: Article 8 clearly states that without prejudice to paragraph 8(2), **no MIF per direct debit transaction** or other agreed remuneration with an equivalent object or effect shall apply to direct debit transactions. Article 8(2) however permits the application of a MIF for R-transactions provided that certain conditions are complied with.²¹⁴ These conditions are as follows:

- the arrangement aims at efficiently allocating costs to the PSP which, or the PSU of which, has caused the R-transaction, as appropriate, while taking into account the existence of transaction costs and ensures that the payer is not automatically charged and the PSP is prohibited from charging PSUs in respect of a given type of R-transaction fees that exceed the cost borne by the PSP for such transactions (Article 8(2)(a));
- the fees are strictly cost based (Article 8(3)(b));

²¹¹ The data elements referred to in Article 5(2)(b) are the following: (i) the payer's name, (ii) the IBAN of the payer's payment account, (iii) the amount of the credit transfer, (iv) the IBAN of the payee's payment account, (v) any remittance information, (vi) any payee identification code, (vii) the name of any payee reference party, (viii) any purpose of the credit transfer, (ix) any category of the purpose of the credit transfer.

²¹² The data elements referred to in Article 5(2)(c) are the following: (i) the payer's name, (ii) the amount of the credit transfer, (iii) any remittance information.

²¹³ See Article 5(4) to 5(8) for additional requirements.

²¹⁴ R-transactions are defined as a payment transaction which cannot be properly executed by a PSP or which results in exception processing, inter alia, because of a lack of funds, revocation, a wrong amount or a wrong date, a lack of mandate or wrong or closed account.

- the level of the fees does not exceed the actual costs of handling an R-transaction by the most cost-efficient comparable PSP that is a representative party to the arrangement in terms of volume of transactions and nature of services (Article 8(3)(c));
- the application of the fees in accordance with points (a), (b) and (c) prevent the PSP from charging additional fees relating to the costs covered by those interchange fees to their respective PSUs (Article 8(3)(d));
- there is no practical and economically viable alternative to the arrangement which would lead to an equally or more efficient handling of R-transactions at equal or lower cost to consumers (Article 8(3)(e)).

Payment accessibility: A payer making a credit transfer to a payee holding a payment account located within the Union is not required to specify the Member State in which that payment account is to be located, provided that the payment account is reachable in accordance with Article 3. Similarly, a payee accepting a credit transfer or using a direct debit to collect funds from a payer holding a payment account located within the Union is not required to specify the Member State in which that payment account is to be located, provided that the payment account is reachable in accordance with Article 3.

Competent authorities: Article 10(1) required Member States to designate as the competent authorities responsible for ensuring compliance with the Regulation, public authorities, bodies recognised by national law or public authorities expressly empowered for that purpose by national law, including national central banks. Member States may designate existing bodies to act as competent authorities. Member States must ensure that the competent authorities have all the powers necessary for the performance of their duties. Where there is more than one competent authority for matters covered by the Regulation, Member States must ensure that those authorities cooperate closely so that they can discharge their respective duties effectively (Article 10(3)).

Penalties: Article 11 required Member States to lay down rules on the penalties applicable to infringements of the Regulation and shall take all measures necessary to ensure that they are implemented by 1 February 2013. Penalties must be effective, proportionate and dissuasive.

Out-of-court complaint and redress procedures: Member States are required in terms of Article 12 to establish adequate and effective out-of-court complaint and redress procedures for the settlement of disputes concerning rights and obligations arising from the Regulation between PSUs and their PSPs. For these purposes, Member States were required to designate existing bodies or where appropriate, set up new bodies and notify the Commission of the applicable bodies by 1 February 2013.

3.2.2 The Directives

Directives are issued by the Council or by the Council together with Parliament (co-decision) and by the Commission. As noted by Mathijsen, directives “constitute the appropriate measure when existing national legislation must be modified or national provisions must be enacted, in most cases for the sake of harmonisation. Directives are binding on Member States to which they are addressed, as to the results to be achieved. Although this means that Member States are obliged to take the national measures necessary to achieve the results set out in the directive, they are free to decide how they transpose this piece of Community legislation into national law.”²¹⁵

²¹⁵ See Mathijsen P A *Guide to European Union Law* (2004).

The first Directive, Directive 98/26/EC Settlement Finality in Payment and Securities Settlement Systems was adopted in May 1998.²¹⁶ As noted in the Commission of the European Communities, "Directive 98/26/EC was the Community legislator's response to the concerns identified by the Committee on Payment and Securities Systems (CPSS) under the auspices of the Bank for International Settlements regarding systemic risk. With the start of stage II of the Economic and Monetary Union (EMU) in 1994, it became evident that there was a need for a stable and efficient payment infrastructure to assist cross-border payments, to support the future single monetary policy and to minimise systemic risk especially in view of the increasing cross-border aspects."²¹⁷ Directive 98/26/EC aimed to reduce the systemic risk associated with participation in payment and securities settlement systems, and in particular the risk linked to the insolvency of a participant in such a system. As noted on the European Commission website, Directive 98/26/CE aims to "contributes to the efficient and cost-effective operation of cross-border payment and securities settlement arrangements, thereby reinforcing the freedom of movement of capital and the freedom to provide services within the internal market."²¹⁸

Directive 1999/93/EC on a Community Framework for Electronic Signatures was, as noted by Wandhöfer, "another helpful attempt to promote the use of electronic payments, particularly in the context of e-commerce as well as to encourage the move to a non-paper environment."²¹⁹ Directive 1999/93/EC introduced criteria for a harmonised basis upon which electronic signatures can be recognised across Europe by focusing on certification services.²²⁰

Directive 2000/46/EC on Electronic Money Institutions was repealed by Directive 2009/110/EC E-Money. The new E-Money Directive aims to enable new, innovative and secure electronic money services to be designed, to provide market access to new companies and to foster real and effective competition between all market participants.

Directive 2000/28/EC on Credit Institutions was passed in 2000. This Directive was however later repealed by Directive 2006/48/EC on Capital Adequacy of Investment Firms and Credit Institutions.²²¹ Directive 2006/48/EC on Capital Adequacy of Investment Firms and Credit Institutions has since been repealed by Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms.

²¹⁶ The Directive entered into force on December 11th, 1999 for the EU 15 Member States and for the 10 new EU Member States on May 1st, 2004.

²¹⁷ See Commission of the European Communities, *Evaluation Report on the Settlement Finality Directive 98/26/EC (EU 25)*.

²¹⁸ See http://ec.europa.eu/internal_market/financial-markets/settlement/dir-98-26-summary_en.htm

²¹⁹ Wandhöfer *EU Payments Integration: The Tale of SEPA, PSD and Other Milestones Along the Road* 39.

²²⁰ 39. Wandhöfer describes certain shortcomings of Directive 1999/93/EC and states, "the law describes an advanced electronic signature, a so-called qualified signature (without however actually precisely defining it – unfortunately not totally unheard of in the era of EU legislation), as something which should legally satisfy the requirements for signing electronic data. The idea was that such an electronic signature should be valid even in the context of legal proceedings, and should be allowed to be used instead of costly handwritten and paper-based procedures to authenticate oneself. The most striking point, besides the lack of definition of the lynchpin of this law (the advanced electronic signature itself), is the fact that Member States were put under the obligation to ensure that all certification providers and national bodies that accredit or supervise them comply with a further, even more complicated and elusive law, the famous Directive 95/46/EC on the protection of personal data."

²²¹ 36. Wandhöfer notes that, "the CAD covers requirements for capital that have to be satisfied by investment firms and credit institutions with a view to limiting risks. This legislation is undergoing regular reviews and extensions and continues to embed the recommendations of the BIS Basel Committee (Last change applied 07/20/2010)."

Directive 2007/64/EC on Payment Services in the Internal Market (The PSD) provides the necessary legal platform for SEPA and is known as the new legal framework for payments (NLF). The aim of the directive is to harmonise legislation pertaining to the provision of payments services within the European Union, increase competition, reinforce consumer protection through transparency of information and charges and define the rights and obligations of payment service providers and their users. The PSD became law on 1 November 2009 and ensures that the rules on electronic payments are the same in 30 European countries (European Union, Iceland, Norway and Liechtenstein). Transposition of the PSD into national legislation was mandated, allowing Member States limited discretion during implementation. Each EU member state has the right to assign whichever regulator or competent authority it defines as the most appropriate to oversee the implementation of the PSD and ensure a successful introduction of the PSD principles into operational practices at the national level.

In the section that follows, best practice principles drawn from several of the directives described above, are presented. In addition, as directives must be transposed into domestic law or regulation, several examples of the approach taken by Member States to do so, are presented.

3.2.2.1 Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC)

Directive 98/26/EC as amended by Directive 2009/44/EC applies to payment and securities settlement systems as well as any participant in such a system and to collateral security provided in connection with the participation in a system, or operations of the central banks of the Member States in their functions as central banks. Directive 98/26/EC as amended by Directive 2009/44/EC contains provisions on:

- designation of Payment and Securities Settlement Systems;
- transfer orders and netting (legal enforceability of transfer orders and netting, irrevocability of transfer orders, no unwinding of netting);
- insolvency proceedings (non-retroactivity of insolvency proceedings, determination of applicable law) and;
- collateral security (e.g. insulation from insolvency proceedings, determination of the law applicable to cross-border provision of collateral security).

Designation of Payment and Securities Settlement Systems: Articles 6 and 10 of Directive 98/26/EC as amended by Directive 2009/44/EC require Member States to notify to the Commission of which systems they have designated and which national authorities are in charge of notification. The Commission holds two registers with this information. They are up-dated whenever Member States send new information to the Commission. Specifically, Article 10(1) reads:

“Member States shall specify the systems, and the respective system operators, which are to be included in the scope of this Directive and shall notify them to the Commission and inform the Commission of the authorities they have chosen in accordance with Article 6(2). The system operator shall indicate to the Member State whose law is applicable the participants in the system, including any possible indirect participants, as well as any change in them. In addition to the indication provided for in the second subparagraph, Member States may impose supervision or authorisation requirements on systems which fall under their jurisdiction. An institution

shall, on request, inform anyone with a legitimate interest of the systems in which it participates and provide information about the main rules governing the functioning of those systems.”²²²

Transfer Orders and Netting: Articles 3, 4 and 5 contain provisions on transfer orders and netting. Article 3(1) provides that transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, provided that transfer orders were entered into the system before the moment of opening of insolvency proceedings as defined in Article 6(1). This applies even in the event of insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant.²²³ Article 3(2) is an override provision and states that “no law, regulation, rule or practice on the setting aside of contracts and transactions concluded before the moment of opening of insolvency proceedings, as defined shall lead to the unwinding of a netting.”

Article 3(4) inserted by Directive 2009/44/EC makes specific reference to interoperable systems and states that each system must determine in its own rules the moment of entry into its system, in such a way as to ensure, to the extent possible, that the rules of all interoperable systems concerned are coordinated. Further, “unless expressly provided for by the rules of all the systems that are party to the interoperable systems, one system’s rules on the moment of entry shall not be affected by any rules of the other systems with which it is interoperable.”

Article 4 permits Member States to provide that the opening of insolvency proceedings against a participant or a system operator of an interoperable system shall not prevent funds or securities available on the settlement account of that participant from being used to fulfil that participant’s obligations in the system or in an interoperable system on the business day of the opening of the insolvency proceedings. Member States may also provide that such a participant’s credit facility connected to the system be used against available, existing collateral security to fulfil that participant’s obligations in the system or in an interoperable system.

Article 5 prohibits a transfer order from being revoked by a participant in a system, nor by a third party, from the moment defined by the rules of that system.²²⁴

Insolvency Proceedings: Insolvency proceedings are covered in Articles 6 to 8 of Directive 98/26/EC. Article 6 defines the moment of opening of insolvency proceedings as the moment when the relevant judicial or administrative authority handed down its decision. The relevant judicial or administrative authority is required

²²² Article 10(2) states that, “a system designated prior to the entry into force of national provisions implementing Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial collateral arrangements as regards linked systems and credit claims shall continue to be designated for the purposes of this Directive. A transfer order which enters a system before the entry into force of national provisions implementing Directive 2009/44/EC, but is settled thereafter shall be deemed to be a transfer order for the purposes of this Directive.”

²²³ The Article states further that “Where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.”

²²⁴ In addition, Article 5 as amended by Directive 2009/44/EC states that, “in the case of interoperable systems, each system determines in its own rules the moment of irrevocability, in such a way as to ensure, to the extent possible, that the rules of all interoperable systems concerned are coordinated in this regard. Unless expressly provided for by the rules of all the systems that are party to the interoperable systems, one system’s rules on the moment of irrevocability shall not be affected by any rules of the other systems with which it is interoperable.”

to immediately notify the appropriate authority chosen by its Member State of the insolvency decision.²²⁵ Member States are also required to immediately notify other Member States of the decision.²²⁶

Article 7 confirms that insolvency proceedings shall not have retroactive effects on the rights and obligations of a participant arising from, or in connection with, its participation in a system before the moment of opening of such proceedings.²²⁷ This applies, inter alia, as regards the rights and obligations of a participant in an interoperable system, or of a system operator of an interoperable system which is not a participant.

Collateral Security: Article 9 of Directive 98/26/EC provides for the insulation of the rights of holders of collateral security from the effects of the insolvency of the provider.²²⁸ The rights of a system operator or of a participant to collateral security provided to them in connection with a system or any interoperable system, and the rights of central banks of the Member States or the European Central Bank to collateral security provided to them, are not affected by insolvency proceedings against:

- (a) the participant (in the system concerned or in an interoperable system);
- (b) the system operator of an interoperable system which is not a participant;
- (c) a counterparty to central banks of the Member States or the European Central Bank; or
- (d) any third party which provided the collateral security.

Article 9(2) reads, "where securities including rights in securities are provided as collateral security to participants, system operators or to central banks of the Member States or the European Central Bank as described in paragraph 1, and their right or that of any nominee, agent or third party acting on their behalf with respect to the securities is legally recorded on a register, account or centralised deposit system located in a Member State, the determination of the rights of such entities as holders of collateral security in relation to those securities shall be governed by the law of that Member State."

As the Settlement Finality Directive 98/26/EC must be transposed into domestic law or regulation, Table 14 below is presented as a reference of the laws and or regulations that were adopted and amendments that were made to existing domestic laws and regulations by several EU Member States to meet this obligation.

[Annexure O](#) of this report provides a detailed example of how the Settlement Finality Directive 98/26/EC was transposed into domestic regulation by Ireland.²²⁹

²²⁵ Article 6(2) of Directive 98/26/EC.

²²⁶ Article 6(3).

²²⁷ As the insolvency of a participant may not have retroactive effects, this amounts to the abolition of "zero hour rules".

²²⁸ Collateral security shall not be affected by insolvency proceedings: if a participant defaults, the system should be able to settle. Collateral security provided to a system by a participant is therefore insulated from insolvency proceedings against that participant.

²²⁹ Parliament adopted the Transposition Act in November 1999; Act became effective on 10 December 1999. Notification to ESA has taken place.

Table 13: Examples of the National Application of Settlement Finality Directive

Member state	State of play of legislative procedure
Belgium	Law adopted as amended on 28.04.99, entry into force: 11.6.1999 Law of 28/4/99 (amended by Royal Decree of 18/8/99) Official Journal 8.9.1999.
Croatia	Act on Settlement Finality in Payment and Financial Instruments Settlement Systems (Official Gazette No. 59/2012, 28 May 2012).
Denmark	Law 117 of 11 April 2000. Official Journal (Lovtidende A) Numero 283 of 26.04.2000.
Germany	Transposition is split into two legislative projects: The contractual aspects of Art. 3-5 of Dir. 98/26/EC are transposed with the credit transfer law (entry into force: 14/8/99) by creating the new §676, §676a Abs3 and 4, §676d Abs2 and §676g Abs1 BGB. The remaining provisions of Dir. 98/26/EC are transposed by <i>Gesetz zur Änderung insolvenzrechtlicher und kreditwesenrechtlicher Vorschriften</i> of 8/12/1999, BGBl. 1999 Teil 1 Nr. 54 of 10/12/1999, p.2384
Spain	Law 41/1999 of 12/11/1999 and published on 13/11/1999 in the OJ (BOE núm. 272; p. 39646 ff). Entry into force on the day after publication in the Official Journal.
France	Transposition in Art. 93 of the Banking Law and in Art. 30 of Law 01/420 of 15 May 2001
Greece	Law 2548/1997 transposes the principles of the Directive into Greek legislation. Law 2789/2000 "Harmonisation of Greek law to the Directive 98/26/EC concerning Settlement Finality and other provisions" (Official Journal of 11/2/2000, entry into force on 11/2/2000) completes the transposition.
Italy	Transposition by Decreto legislativo n. 210 of 12 April 2001; published in gazzetta ufficiale No. 130 of 7 June 2001
Ireland	Implementation by Statutory Instrument No 539 of 1998, European Communities (Finality of Settlement in Payment and Securities Settlement Systems) Regulations, 1998; entry into force: 4/1/1999
Luxembourg	Law of 12.1.2001. It is amending the law of 5.4.1993 on the financial sector. Publication in the Mémorial on 6.2.2001. Entry into force on 10.2.2001.
Netherlands	Law of 17.12.1998; in force since 01.01.1999. (Staatsblad n° 714)
Austria	Adoption by Parliament on 22 July 1999: Bundesgesetz 123 - Überweisungs-gesetz (BGBl of 22.7.1999, Part I, page 159); same law transposes Dir. 97/5/EC), Entry into force:10/12/1999
Portugal	Decreto-Lei No. 486/99 of 13/11/1999; Publication in Official Journal Numero 265 of 13/11/1999, pp. 7968, and Decreto-Lei No. 221/2000 of 9/9/2000; publication in Official Journal Numero 209 of 9/9/2000, pp.4783.
Sweden	Legislative measures [Law (1999:1309), Law (1999:1310), Law (1999:1311), Regulation (1999:1312), Regulation (1999:1313), Regulation (1999:1314) in force since 1/1/2000.
Finland	Implementing Law has been adopted on 9/11/1999; entry into force on 11.12.1999 Act on Certain Conditions on Securities and Currency Dealing and Settlement Systems (1084/1999); Statutes of Finland, 2.12.1999; Act on the amendment of Article 5a of the Act on Book-entry Accounts (1085/1999); Statutes of Finland 2.12.1999; Account Transfer Act (821/1999), Article 18, paragraph 2; - Bankruptcy Act (110/1995), Article 76
United Kingdom	The Financial Markets and Insolvency (Settlement Finality) Regulations 1999 Numero 2979 of 2.11.1999 Entry into force: 11/12/1999

Liechtenstein	Team of government experts are presently clarifying which points of the directive would be of relevance for an implementation
Norway	Act on Payment Systems entered into force on 14/4/2000
Iceland	Parliament adopted the Transposition Act in November 1999; Act became effective on 10 December 1999. Notification to ESA has taken place.

Source: European Commission²³⁰

3.2.2.2 Electronic Signatures Directive 1999/93/EC

Directive 1999/93/EC established the legal framework at European level for electronic signatures and certification services, thereby allowing the free flow of electronic signature products and services across borders and ensuring a basic legal recognition of electronic signatures. The three forms of electronic signature that the Directive addresses are:

- the simplest form of the "electronic signature" which serves to identify and authenticate data (as simple as signing an e-mail message with a person's name or using a PIN-code)²³¹;
- the "advanced electronic signature"(which uses encryption technology to sign data, and requires a public and a private key)²³²;
- the "qualified electronic signature" (an advanced electronic signature based on certification and the use of a secure-signature-creation device that has to comply with the requirements in Annex I, II and III of the Directive, which aims to meet the legal requirements of a hand written signature).²³³

Legal Effects of Electronic Signatures: Article 5(1) of Directive 1999/93/EC requires Member States to ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legal proceedings. Secure-signature-creation devices must meet the requirements laid down in Annex III.

Article 5(2) requires Member States to ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device.

²³⁰ See http://ec.europa.eu/internal_market/financial-markets/settlement/dir-g8-26-implementation_en.htm

²³¹ 'Electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication (Article 2(1)).

²³² An advanced electronic signature is defined as an, "electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (Article 1(2))."

²³³ Annex 1 sets out the requirements for qualified certificates, Annex II the requirements for certification-service-providers issuing qualified certificates and Annex III, the requirements for secure signature-creation devices.

Liability of a Certification Service-provider: Member States must ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

- as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate (Article 6(1)(a));
- for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature verification data given or identified in the certificate (Article 6(1)(b));
- for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both (Article 6(1)(c)); unless the certification-service-provider proves that he has not acted negligently.

International Validity: Article 7 covers the validity international validity of qualified certificates issued in one Member State by a certification service provider, in another Member State. Member States are required to ensure that certificates which are issued as qualified certificates to the public by a certification service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification service provider established within the Community if a number of conditions are fulfilled.²³⁴

Data Protection: Member States are required to ensure that certification-service providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Article 8(1)). As such, Member States must ensure that a certification-service provider that issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject (Article 8(2)).

As the Electronic Signatures Directive 1999/93/EC must be transposed into domestic law or regulation, Table 15 below is presented as a reference of the laws and or regulations that were adopted and amendments that were made to existing domestic laws and regulations by several EU Member States to meet this obligation.

Annexure P of this report provides a detailed example of how the Electronic Signatures Directive 1999/93/EC was transposed into domestic law and regulation by the United Kingdom.²³⁵

²³⁴ These requirements are as follows: (a) the certification-service-provider fulfills the requirements laid down in the Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) a certification-service-provider established within the Community which fulfills the requirements laid down in the Directive guarantees the certificate; or (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

²³⁵ The Electronic Signatures Regulations, 2002 S.I. n° 318 of 2002, came into force on 08/03/2002

Table 14: Examples of the National Application of Electronic Signatures Directive

Member state	State of play of legislative procedure
France	<ul style="list-style-type: none"> • Loi n° 2004/801 du 6/8/2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78 -17 du 6/1/1978 relative à l'informatique, aux fichiers et aux libertés. • Legal act: Loi, number: 2004/801; Official Journal: Journal Officiel de la République Française (JORF), number: 2004/182, Publication date: 07/08/2004, Page: 14063-14063; Reference: (MNE(2004)51672) • Loi n° 575 du 21/6/2004 pour la confiance dans l'économie numérique. • Legal act: Loi, number: 575; Official Journal: Journal Officiel de la République Française (JORF), Publication date: 22/06/2004, Page: 00001-00022; Reference: (MNE(2004)50105) • Arrêté du 31/05/2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation JORF du 08/06/2002 p. 10223 (NOR : ECOI0200314A) (SG(2003)A/47 du 09/01/2003) • Legal act: Arrêté; Official Journal: Journal Officiel de la République Française (JORF), Publication date: 08/06/2002, Page: 10223 • Décret 2001-272 du 30 mars 2001 - Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, entrée en vigueur le 31/03/2001 JORF du 31/03/2001, page 5070 (NOR JUSCO12O141D) • Legal act: Décret, number: 2001-272; Official Journal: Journal Officiel de la République Française (JORF), Publication date: 31/03/2001, Page: 5070, Entry into force: 30/03/2001 • Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique JORF n° 62 du 14/03/2000, page 3968 (NOR JUSX9900020L) • Legal act: Loi, number: 2000-230; Official Journal: Journal Officiel de la République Française (JORF), number: 62, Publication date: 14/03/2000, Page: 3968, Entry into force: 13/03/2000; Reference: (SG(2001)A/09077)
Netherlands	<ul style="list-style-type: none"> • Regeling van de Staatssecretaris van Economische Zaken van 6/5/2003, n° WJZ/03/02263, houdende nadere regels met betrekking tot elektronische handtekeningen (Regeling elektronische handtekeningen). ref: Staatscourant n° 88

	<p>van 8/5/2003 p. 9</p> <ul style="list-style-type: none"> • Legal act: Regeling; Official Journal: Administrative measures; Reference: (SG(2003)A/05810) • Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatie dienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 8.16 van de Telecommunicatiewet (Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen)), gepubliceerd in de Staatscourant van 8 mei 2003, nr 88. • Legal act: Wet; Official Journal: Administrative measures • Besluit van 8/5/2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen (Besluit elektronische handtekeningen). ref: Staatsblad n° 200 van 20/5/2003 • Legal act: Besluit; Official Journal: Administrative measures • Wet van 8/5/2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn n° 1999/93/EG van 13/12/1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen). ref: Staatsblad n° 199 van 20/5/2003 • Legal act: Wet; Official Journal: Administrative measures, Entry into force: 13/12/1999
Portugal	<ul style="list-style-type: none"> • Decreto-Lei n° 62/2003 <i>Diario da Republica I Serie A n° 79 du 03/04/2003 p. 2170</i> • Legal act: <i>Decreto-Lei, number: 62/2003; Official Journal: Diaro da Republica I, number: serie A nr 79, Publication date: 03/04/2003; Reference: (SG(2003)A/04008)</i>
Ireland	<ul style="list-style-type: none"> • Electronic Commerce Act, 2000 • Official Journal: Iris Oifigiúil, Entry into force: 20/09/2000; Reference: (SG(2001)A/13903)
United Kingdom	<ul style="list-style-type: none"> • The Electronic Signatures Regulations, 2002 S.I. n° 318 of 2002, came into force on 08/03/2002 • Legal act: Administrative measures; Official Journal: Her Majesty's Stationery Office (HMSO), Publication date: 08/03/2002; Reference: (SG(2002)A/02428)

3.2.2.3 Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amends Directives 2005/60/EC²³⁶ and 2006/48/EC²³⁷ and repeals Directive 2000/46/EC²³⁸. Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions was adopted in response to the emergence of new pre-paid electronic payment products and was intended to create a clear legal framework designed to strengthen the internal market while ensuring an adequate level of prudential supervision.²³⁹ In its review of Directive 2000/46/EC the Commission highlighted the need to revise the first electronic-money Directive since some of its provisions were considered to have hindered the emergence of a true single market for electronic money services and the development of such user-friendly services.²⁴⁰

It is important to note that the application of Directive 2009/110/EC is limited to payment service providers that issue electronic money.²⁴¹

“Electronic money” means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer (Article 2(2)).”

The Directive does not apply to monetary value stored on specific pre-paid instruments, designed to address precise needs that can be used only in a limited way, because they allow the electronic money holder to purchase goods or services only in the premises of the electronic money issuer or within a limited network of service providers under direct commercial agreement with a professional issuer, or because they can be used only to acquire a limited range of goods or services (Recital 5).²⁴² The Directive is also not applicable to monetary value that is used to purchase digital goods or services, where, by virtue of the nature of the good or service, the operator adds intrinsic value to it, e.g. in the form of access, search or distribution facilities, provided that the good or service in question can be used only through a digital device, such as a mobile phone or a computer, and provided that the telecommunication, digital or information technology operator does not act only as an intermediary between the payment service user and the supplier of the goods and services (Recital 6).²⁴³

²³⁶ Directive on the Use of the Financial System for the Purpose of Money Laundering – Third AML Directive.

²³⁷ Directive on Capital Adequacy of Investment Firms and Credit Institutions.

²³⁸ Directive on Electronic Money Institutions.

²³⁹ Recital 1 of Directive 2009/110/EC.

²⁴⁰ Recital 2.

²⁴¹ Recital 3.

²⁴² Recital 5 states further that, “an instrument should be considered to be used within such a limited network if it can be used only either for the purchase of goods and services in a specific store or chain of stores, or for a limited range of goods or services, regardless of the geographical location of the point of sale. Such instruments could include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services (such as vouchers for childcare, or vouchers for social or services schemes which subsidise the employment of staff to carry out household tasks such as cleaning, ironing or gardening), which are sometimes subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation.”

²⁴³ Recital 6 states further that, “this is a situation where a mobile phone or other digital network subscriber pays the network operator directly and there is neither a direct payment relationship nor a direct debtor-creditor relationship between the network subscriber and any third-party supplier of goods or services delivered as part of the transaction.”

Recital 13 clarifies the European Parliament and the Council's view that the issuance of electronic money does not constitute deposit-taking. Specifically, Recital 13 reads,

“the issuance of electronic money does not constitute a deposit-taking activity pursuant to Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, in view of its specific character as an electronic surrogate for coins and banknotes, which is to be used for making payments, usually of limited amount and not as means of saving. Electronic money institutions should not be allowed to grant credit from the funds received or held for the purpose of issuing electronic money. Electronic money issuers should not, moreover, be allowed to grant interest or any other benefit unless those benefits are not related to the length of time during which the electronic money holder holds electronic money. The conditions for granting and maintaining authorisation as electronic money institutions should include prudential requirements that are proportionate to the operational and financial risks faced by such bodies in the course of their business related to the issuance of electronic money, independently of any other commercial activities carried out by the electronic money institution.”

The issuance of E-Money is limited to credit institutions authorised in accordance with Directive 2006/48/EC, post office giro institutions entitled under national law to issue electronic money, institutions referred to in Article 2 of Directive 2006/48/EC, the European Central Bank, national central banks when not acting in their capacity as monetary authority or other public authorities and Member States or their regional or local authorities when acting in their capacity as public authorities (Recital 17).

Member States are permitted to waive the application of all or part of the provisions of Title II of the Directive to the institutions referred to in Article 2 of Directive 2006/48/EC, with the exception of those referred to in the first and second indents of that Article.²⁴⁴

General Prudential Rules: Article 3 sets out the general prudential rules applicable to E-Money institutions. Article 3(2) requires electronic money institutions to inform the competent authorities in advance of any material change in measures taken for safeguarding of funds that have been received in exchange for electronic money issued. Article 3(4) permits Member States to allow electronic money institutions to distribute and redeem electronic money through natural or legal persons that act on their behalf. Where the electronic money institution wishes to distribute electronic money in another Member State by engaging such a natural or legal person, it is required to follow the procedure set out in Article 25 of Directive 2007/64/EC. However, notwithstanding Article 3(4), electronic money institutions may not issue electronic money through agents. Electronic money institutions are allowed to provide payment services referred to in Article 6(1)(a) through agents only if the conditions in Article 17 of Directive 2007/64/EC are met.²⁴⁵

Initial Capital: As per Article 4, Member States must require electronic money institutions to hold, at the time of authorisation, initial capital, comprised of the items set out in Article 57(a) and (b) of Directive 2006/48/EC, of not less than EUR 350 000.²⁴⁶

²⁴⁴ Article 1(3) Directive 2009/110/EC.

²⁴⁵ Article 3(5).

²⁴⁶ Article 57(a) and (b) of Directive 2006/48/EC read, “subject to the limits imposed in Article 66, the unconsolidated own funds of credit institutions shall consist of the following items: (a) capital within the meaning of Article 22 of Directive 86/635/EEC, in so far as it has been paid up, plus share premium accounts but excluding cumulative preferential shares; (b) reserves within the meaning of Article 23 of Directive 86/635/EEC and profits and losses brought forward as a result of the application of the final profit or loss.”

Own Funds: The electronic money institution’s own funds, as set out in Articles 57 to 61, 63, 64 and 66 of Directive 2006/48/EC must not fall below the amount required under paragraphs 2 to 5 of Article 5 or under Article 4 of this Directive, whichever the higher.

Activities: Article 6 sets out the activities that electronic money issuers may engage in. These activities are in addition to the issuing of electronic money and are set out in Table 15 below.

Table 15: Activities that Electronic Money Issuers May Engage In

Article	Listed Activity
6(1)(a)	The provision of payment services listed in the Annex to Directive 2007/64/EC. (See section xx below).
6(1)(b)	The granting of credit related to payment services referred to in points 4, 5 or 7 of the Annex to Directive 2007/64/EC, where the conditions laid down in Article 16(3) and (5) of that Directive are met. ²⁴⁷
6(1)(c)	The provision of operational services and closely related ancillary services in respect of the issuing of electronic money or to the provision of payment services referred to in 6(1)(a).
6(1)(d)	The operation of payment systems as defined in point 6 of Article 4 of Directive 2007/64/EC and without prejudice to Article 28 of that Directive.
6(1)(e)	Business activities other than issuance of electronic money, having regard to the applicable Community and national law.

Article 6(2) makes it quite clear that electronic money institutions may not take deposits or other repayable funds from the public within the meaning of Article 5 of Directive 2006/48/EC.²⁴⁸ As such, any funds received by electronic money institutions from the electronic money holder must be exchanged for electronic money without delay. Such funds do not constitute either a deposit or other repayable funds received from the public within the meaning of Article 5 of Directive 2006/48/EC.²⁴⁹

Safeguarding Requirements: Member States must require electronic money institutions to safeguard funds that have been received in exchange for electronic money issued. This is in accordance with Article 9(1) and (2) of Directive 2007/64/EC. Funds received in the form of payment by payment instrument need not be safeguarded until they are credited to the electronic money institution’s payment account or are otherwise made available to the electronic money institution in accordance with the execution time requirements laid down in the Directive 2007/64/EC, where applicable. In any event, such funds must be safeguarded by no later than five business days after the issuance of electronic money.²⁵⁰

Optional Exemptions (Small Electronic Money Institutions): Member States may waive or allow their competent authorities to waive the application of all or part of the procedures and conditions set out in Articles

²⁴⁷ It is important to note that the credit referred to in 6(1)(b) may not be granted from the funds received in exchange of electronic money and held in accordance with Article 7(1).

²⁴⁸ Article 5 of Directive 2006/48/EC reads, “Member States shall prohibit persons or undertakings that are not credit institutions from carrying on the business of taking deposits or other repayable funds from the public. The first paragraph shall not apply to the taking of deposits or other funds repayable by a Member State or by a Member State’s regional or local authorities or by public international bodies of which one or more Member States are members or to cases expressly covered by national or Community legislation, provided that those activities are subject to regulations and controls intended to protect depositors and investors and applicable to those cases.”

²⁴⁹ Article 6(3) Directive 2009/110/EC.

²⁵⁰ Article 7(1).

3, 4, 5 and 7 of Directive 2009/110/EC, with the exception of Articles 20, 22, 23 and 24 of Directive 2007/64/EC, and allow legal persons to be entered in the register for electronic money institutions if both of the following requirements are complied with:

- (a) the total business activities generate an average outstanding electronic money that does not exceed a limit set by the Member State but that, in any event, amounts to no more than EUR 5 000 000; and
- (b) none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes.²⁵¹ Member States may also provide for the granting of the optional exemptions under Article 9 to be subject to an additional requirement of a maximum storage amount on the payment instrument or payment account of the consumer where the electronic money is stored.

Issuance and Redeemability: Electronic money must be issued at par value on the receipt of funds.²⁵² The contract between the electronic money issuer and the electronic money holder must clearly and prominently state the conditions of redemption, including any fees relating thereto, and the electronic money holder shall be informed of those conditions before being bound by any contract or offer.²⁵³ Redemption may be subject to a fee only if stated in the contract and only in any of the following cases: (a) where redemption is requested before the termination of the contract; (b) where the contract provides for a termination date and the electronic money holder terminates the contract before that date; or (c) where redemption is requested more than one year after the date of termination of the contract. These fees must be proportionate and commensurate with the actual costs incurred by the electronic money issuer.²⁵⁴

Prohibition of Interest: Electronic money Issuers are prohibited from the granting of interest or any other benefit related to the length of time during which an electronic money holder holds the electronic money.²⁵⁵

As the Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions must be transposed into domestic law or regulation, Table 16 below is presented as a reference of the laws and or regulations that were adopted and amendments that were made to existing domestic laws and regulations by several EU Member States to meet this obligation.

[Annexure Q](#) of this report provides a detailed example of how Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions was transposed into domestic law and regulation by Ireland.²⁵⁶

²⁵¹ Article 9(1).

²⁵² Article 11(1).

²⁵³ Article 11(3).

²⁵⁴ Article 11(4).

²⁵⁵ Article 12 Directive.

²⁵⁶ See the European Communities (Electronic Money) Regulations 2011 (S.I. No. 183 of 2011).

Table 16: Examples of the National Application of the E-Money Directive

Member State	National Application of E-Money Directive
France	Loi n° 2013-100 du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière bancaire et financière ²⁵⁷
Netherlands	<ul style="list-style-type: none"> • 670 Wet van 22 December 2011 tot wijziging van de Wet op het financieel toezicht en enige andere wetten ter implementatie van richtlijn nr. 2009/110/EG van het Europees Parlement en de Raad betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronische geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PbEU L 267)²⁵⁸ • 673 Besluit van 22 December 2011, houdende wijziging van enkele algemene maatregelen van bestuur op het gebied van het financieel toezicht in verband met de implementatie van richtlijn nr. 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PbEU L 267)²⁵⁹ • Besluit van 22 Juni 2011 tot wijziging van het Besluit Gedragstoezicht financiële ondernemingen Wft in verband met de implementatie van titel III van richtlijn nr. 2009/110/EG van het Europees Parlement en de Raad van de Europese Unie van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van richtlijn 2000/46/EG (Pb EU L 267)²⁶⁰ • Wijziging van de Vrijstellingsregeling Wft in verband met de implementatie van

²⁵⁷ Law n° 2013-100 of 28 January 2013. It amends the Monetary and Financial Code and transposes in particular Directives 2009/110/EC, 2011/7/EU and 2010/78/EU. As Law n° 2013-100 is a legislative act, it only transposes legislative provisions in accordance with the division between legislative and regulatory competences under French law. As a result, it requires the adoption of Decrees and Orders to complete its provisions and ensure full transposition of the Directive. However, at the time of this assessment, the regulatory acts completing this Law were not adopted.

²⁵⁸ 670 Act of 22 December 2011 amending the Financial Supervision Act and other laws for the transposition of Directive 2009/110/EC of the European Parliament and the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (PbEU L 267).

²⁵⁹ 673 Decree of 22 December 2011 amending other Orders of Decree concerning financial supervision in connection with the transposition of Directive 2009/110/EC of the European Parliament and the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC.

²⁶⁰ Decree of 22 June 2011 amending the Decree Conduct Supervision Financial Undertakings of the Financial Supervision Act in connection with the implementation of Title III of Directive 2009/110/EC of the European Parliament and the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (PbEU L 267).

	richtlijn 2009/110/EG van het Europees Parlement en de Raad betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PbEU L 267) ²⁶¹
Portugal	<ul style="list-style-type: none"> • Decreto-Lei n.º 242/2012. D.R. n.º 215, Série I de 07 de Novembro 2012 • Lei n.º 34/2012. D.R. n.º 163, Série I de 23 Agosto 2012 • Regime Geral das Instituições de Crédito e Sociedades Financeiras (Aprovado pelo Decreto-Lei nº 298/92, de 31 de Dezembro e alterado posteriormente)
Ireland	<ul style="list-style-type: none"> • The European Communities (Electronic Money) Regulations 2011 (S.I. No. 183 of 2011)
United Kingdom	<ul style="list-style-type: none"> • The Electronic Money Regulations 2011 S.I. 2011/99 • The Financial Services (Electronic Money) Regulations 2011 (Gibraltar Gazette No. 3879 of 29 September 2011, LN. 2011/167)

3.2.2.4 Directive 2004/39/EC Markets in Financial Instruments (MiFID)

Directive 2004/39/EC on Markets in Financial Instruments (which is currently under review) was adopted by the Council of Ministers in April 2004.²⁶² MiFID establishes a comprehensive regulatory framework governing the organised execution of investors' transactions by exchanges, other trading systems and investment firms. Article 34(1) which deals with access to central counterparty, clearing and settlement facilities and right to designate settlement system binds Member States to require that investment firms from other Member States have the right of access to central counterparty, clearing and settlement systems in their territory for the purposes of finalising or arranging the finalisation of transactions in financial instruments. Member States must require that access of those investment firms to such facilities be subject to the same non-discriminatory, transparent and objective criteria as apply to local participants and are prohibited from restricting the use of those facilities to the clearing and settlement of transactions in financial instruments undertaken on a regulated market or multilateral trading facility (MTF) in their territory. Investment firms that wish to participate directly in other Member States' settlement systems must comply with the relevant operational and commercial requirements governing membership, as well as the prudential measures necessary for the smooth and orderly functioning of the relevant financial markets.²⁶³

²⁶¹ Amendment of the Rules on Exemptions of the Financial Supervision Act in connection with the transposition of Directive 2009/110/EC of the European Parliament and the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (PbEU L 267).

²⁶² MiFID was adopted in accordance with the "Lamfalussy" process and consists of a framework Directive (Directive 2004/39/EC)², an implementing Directive (Directive 2006/73/EC)³ and an implementing Regulation (Regulation No 1287/2006).

²⁶³ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 238.

3.2.2.5 Directive 2007/64/EC Payment Services in the Internal Market (PSD)

Directive 2007/64/EC Payment Services in the Internal Market (PSD) otherwise known as the Payment Services Directive was adopted by the European Parliament and the Council in November 2007 and Member States had until 1 November 2009 to transpose the Directive into National Law. As noted by Kokkola, “the Directive aims to create a harmonised legal framework for payments (seeking in particular to establish a legal basis for SEPA), thereby ensuring that cross-border payments within the European Union (particularly credit transfers, direct debits and card payments) can be carried out just as easily, efficiently and securely as domestic payments within the various Member States. It also establishes the concept of “payment institutions” – licensed payment service providers that are able to provide payment services across the European Union under lighter supervisory regime than banks. By opening up the market in this way, the European legislator is seeking to allow new service providers to compete with existing participants on a level playing field, thereby facilitating greater competition.”²⁶⁴

Recital 1 of the PSD affirms that it is essential for the establishment of the internal market that all internal frontiers in the Community be dismantled so as to enable the free movement of goods, persons, services and capital. In this regard, the proper operation of the single market in payment services is vital.²⁶⁵ Recital 5 notes that a legal framework for payment services should ensure the coordination of national provisions on prudential requirements, the access of new payment service providers to the market, information requirements, and the respective rights and obligations of payment services users and providers.

TITLE I SUBJECT MATTER, SCOPE AND DEFINITIONS

3.2.2.5.1 Subject Matter of the Directive

The PSD lays down the rules in accordance with which Member States must distinguish between the following six categories of payment service provider:

- Credit institutions within the meaning of Article 4(1)(a) of Directive 2006/48/EC (Article 1(1)(a));
- Electronic money institutions within the meaning of Article 1(3)(a) of Directive 2000/46/EC (Article 1(1)(b));
- Post Office Giro institutions which are entitled under national law to provide payment services (Article 1(1)(c));
- Payment institutions within the meaning of this Directive (Article 1(1)(d));
- The European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities (Article 1(1)(e));
- Member States or their regional or local authorities when not acting in their capacity as public authorities (Article 1(1)(f)).²⁶⁶

²⁶⁴ See Rambure D and Nacamuli N *Payment Systems: From the Salt Mines to the Board Room* (2008) 79 where the authors note that, “the PSD opens the door for non-banks to provide payment services, either as a sole activity or alongside their core business, such as mobile telephone operators: these PSPs, designated Payment Institutions (PI), will be subject to much lighter capital requirements and regulatory supervision than credit institutions which, as could be expected, met with some resistance from the banking sector. The supervision of these PIs is left to the discretion of each Member State and they can offer their services throughout the EU if authorised by one Member State (*EU passporting principle*).”

²⁶⁵ At the time the Directive was adopted, the payment services markets of the Member States were organised separately, along national lines and the legal framework for payment services was fragmented into 27 national legal systems.

²⁶⁶ Article 1(a) to Article 1(f) Directive 2007/64/EC.

The PSD applies to payment services provided within the Community.²⁶⁷ The payment services falling within the scope of the PSD are listed in the Annex and summarised in Table 17 below.

Table 17: Payment Services to which the PSD applies (“The Annex”)

Payment Services within Scope	
✓	1) Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.
✓	2) Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.
✓	3) Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: <ul style="list-style-type: none"> • execution of direct debits, including one-off direct debits; • execution of payment transactions through a payment card or a similar device; • execution of credit transfers, including standing orders.
✓	4) Execution of payment transactions where the funds are covered by a credit line for a payment service user: <ul style="list-style-type: none"> • execution of direct debits, including one-off direct debits; • execution of payment transactions through a payment card or a similar device; • execution of credit transfers, including standing orders.
✓	5) Issuing and/or acquiring of payment instruments
✓	6) Money remittance
✓	7) Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

The PSD does not however apply to the types of transactions listed in Table 18 below.

Table 18: Negative Application of the PSD

Negative Application	
✗	Payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention
✗	Payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee.
✗	Professional physical transport of banknotes and coins, including their collection, processing and delivery.
✗	Payment transactions consisting of the non-professional cash collection and delivery within the framework of a nonprofit or charitable activity.

²⁶⁷ However, with the exception of Article 73, Titles III and IV shall apply only where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located in the Community. Titles III and IV shall apply to payment services made in euro or the currency of a Member State outside the euro area. Member States may waive the application of all or part of the provisions of this Directive to the institutions referred to in Article 2 of Directive 2006/48/EC, with the exception of those referred to in the first and second indent of that article.

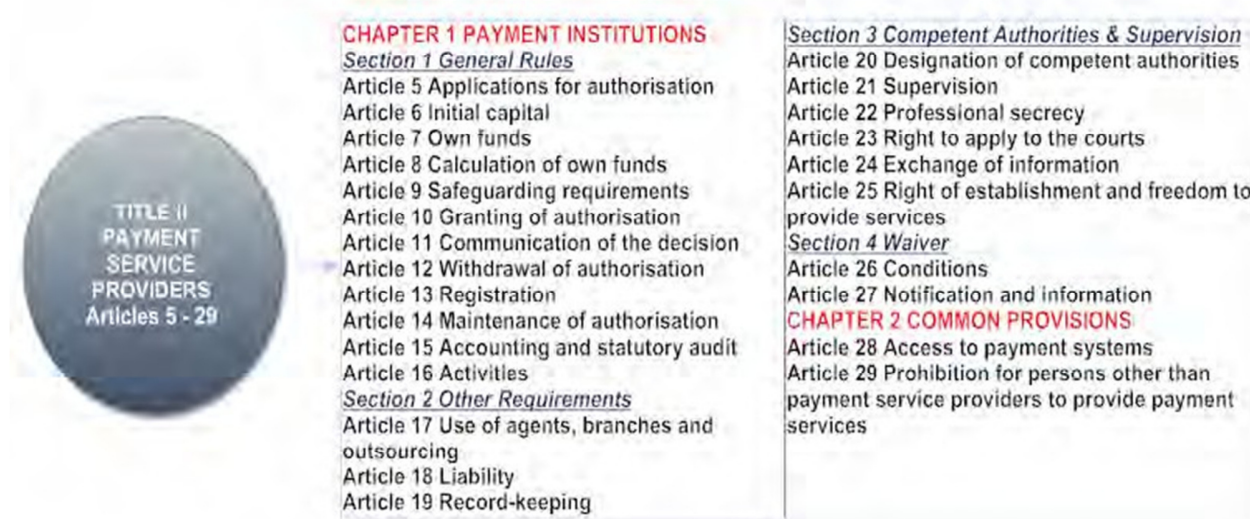
x	Services where the payee provides cash to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services.
x	Money exchange business, that is to say, cash-to-cash operations, where the funds are not held on a payment account.
x	Payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee: <ul style="list-style-type: none"> • Paper cheques; • Paper-based drafts; • Paper-based vouchers; • Paper-based traveller's cheques; or • Paper-based postal money orders.
x	Payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to Article 28.
x	Payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments.
x	Services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services.
x	Services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services.
x	Payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.
x	Payment transactions carried out between payment service providers, their agents or branches for their own account.
x	Payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group.
x	Services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex.

TITLE II PAYMENT SERVICE PROVIDERS

Title II of the PSD covers the general rules applicable to payment service providers, the designation of competent authorities, supervision, the conditions for the application of the permitted waiver and two common provisions, namely, access to payment systems and prohibition for persons other than payment

service providers to provide payment services. The individual articles under each chapter are schematically presented in Diagram 5 below.

Diagram 5: Content of Title II



3.2.2.5.2 Application for Authorisation as a Payment Institution

A payment institutions is defined as, “a legal person that has been granted authorisation in accordance with Article 10 to provide and execute payment services throughout the Community. The application for authorisation as a payment institution must be submitted to the competent authorities of the home Member State, together with the information and documentation listed in Article 5(a) to 5(l).²⁶⁸

3.2.2.5.3 Initial Capital

Article 6 sets out the initial capital requirements. Member States are required to require payment institutions to hold, at the time of authorisation, initial capital, comprised of:

²⁶⁸ This includes, a programme of operations, setting out in particular the type of payment services envisaged; business plan; evidence that the payment institution holds required initial capital, for the payment institutions referred to in Article 9(1), a description of the measures taken for safeguarding payment service users' funds in accordance with Article 9; a description of the applicant's governance arrangements and internal control mechanisms; a description of the internal control mechanisms which the applicant has established in order to comply with obligations in relation to money laundering and terrorist financing under Directive 2005/60/EC and Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds; a description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of its participation in a national or international payment system; the identity of persons holding in the applicant, directly or indirectly, qualifying holdings; the identity of directors and persons responsible for the management of the payment institution; the identity of statutory auditors and audit firms; the applicant's legal status and articles of association; and; the address of the applicant's head office.

- where the payment institution provides only money remittances, its capital shall at no time be less than EUR 20 000;
- where the payment institution provides the payment service listed in point 7 of the Annex, its capital shall at no time be less than EUR 50 000;²⁶⁹
- where the payment institution provides any of the payment services listed in points 1 to 5 of the Annex, its capital shall at no time be less than EUR 125 000.

3.2.2.5.4 *Own Funds*

Article 7 states that, “the payment institution's own funds, as defined in Articles 57 to 61, 63, 64 and 66 of Directive 2006/48/EC, may not fall below the amount required under Articles 6 or 8 of this Directive, whichever the higher.”²⁷⁰ Article 8 provides several methods for the calculation of own funds.

3.2.2.5.5 *Safeguarding Requirements*

Member States or competent authorities are required to require a payment institution which provides any of the payment services listed in the Annex and, at the same time, is engaged in other business activities referred to in Article 16(1)(c) to safeguard funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions.²⁷¹ Two options for safeguarding funds are provided. These are:

Option 1) funds received from the payment service user may not be commingled at any time with the funds of any natural or legal person other than payment service users on whose behalf the funds are held and, where they are still held by the payment institution and not yet delivered to the payee or transferred to another payment service provider by the end of the business day following the day when the funds have been received, they shall be deposited in a separate account in a credit institution or invested in secure, liquid low-risk assets as defined by the competent authorities of the home Member State and they must be insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution, in particular in the event of insolvency.

Option 2) funds received from the payment service user must be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which would have been segregated in the absence of the insurance policy or other comparable guarantee, payable in the event that the payment institution is unable to meet its financial obligations.

²⁶⁹ Point 7 of the Annex reads as follows, “Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.”

²⁷⁰ Directive 2006/48/EC Capital Adequacy of Investment Firms and Credit Institutions.

²⁷¹ The activities listed in Article 16(1)(c) are as follows: (a) the provision of operational and closely related ancillary services such as ensuring the execution of payment transactions, foreign exchange services, safekeeping activities, and the storage and processing of data; (b) the operation of payment systems, without prejudice to Article 28; (c) business activities other than the provision of payment services, having regard to applicable Community and national law.

It is important to note that in terms of Article 9(3), Member States or competent authorities are permitted to require that payment institutions which are not engaged in other business activities referred to in Article 16(1)(c) comply with the safeguarding requirements under paragraph 1 of this Article.

The Member States or competent authorities are also permitted to limit safeguarding requirements to funds of those payment service users whose funds individually exceed a threshold of EUR 600.

3.2.2.5.6 Granting of Authorisation

Member States must require a payment institution that intend to provide payment services, to obtain authorisation as a payment institution before commencing the provision of such payment services. An authorisation is only granted to a legal person established in a Member State (Article 10).²⁷²

3.2.2.5.7 Withdrawal of Authorisation

Authorisation may be withdrawn under the circumstances listed in Article 12. These are: where the payment institution does not make use of the authorisation within 12 months expressly renounces the authorisation or has ceased to engage in business for more than six months, if the Member State concerned has made no provision for the authorisation to lapse in such cases; has obtained the authorisation through false statements or any other irregular means; no longer fulfils the conditions for granting the authorisation; would constitute a threat to the stability of the payment system by continuing its payment services business; or falls within one of the other cases where national law provides for withdrawal of an authorisation.

3.2.2.5.8 Public Register of Authorised Payment Institutions, their Agents and Branches

Article 13 requires Member States to establish a public register of authorised payment institutions, their agents and branches, as well as of natural and legal persons, their agents and branches, benefiting from a waiver under Article 26, and of the institutions referred to in Article 2(3) that are entitled under national law to provide payment services. The register must identify payment services for which the payment institution is authorised or for which the natural or legal person has been registered. The register must be publicly available for consultation, accessible online, and updated on a regular basis.

3.2.2.5.9 Accounting and Statutory Audit

Payment institutions must, in compliance with Article 15(2) have their annual accounts and audited by statutory auditors or audit firms.

3.2.2.5.10 Use of Agents, Branches or Entities to which Activities are Outsourced

²⁷² Article 11 requires competent authorities to, within three months of receipt of an application whether the authorisation has been granted or refused. Reasons must be given whenever an authorisation is refused.

Article 17 of the PSD deals with agents. In terms of Article 17(1), when a payment institution intends to provide payment services through an agent it is required to communicate the following information to the competent authorities in its home Member State:

- the name and address of the agent;
- a description of the internal control mechanisms that will be used by agents in order to comply with the obligations in relation to money laundering and terrorist financing under Directive 2005/60/EC; and
- the identity of directors and persons responsible for the management of the agent to be used in the provision of payment services and evidence that they are fit and proper persons.

Once this information is received, the competent authorities may list the agent in the register provided for in Article 13. However, before listing the agent in the register, the competent authorities may, if they consider that the information provided to them is incorrect, take further action to verify the information. If, after taking action to verify the information, the competent authorities are not satisfied that the information provided to them is correct, they are required to refuse to list the agent in the register

If a payment institution intends to outsource its operational functions it is required to inform the competent authorities of its home Member State accordingly (Article 17(7)).²⁷³

3.2.2.5.11 *Liability*

Article 18 requires Member States to ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of the Directive are complied with. Additionally, Member States must require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced.

3.2.2.5.12 *Record Keeping*

Member States must require payment institutions to keep all appropriate records for the purpose of Title II for at least five years, without prejudice to Directive 2005/60/EC or other relevant Community or national legislation.

3.2.2.5.13 *Designation of Competent Authorities*

Article 20 sets out the requirement of designation of competent authorities. In terms of this article, Member States are required to designate as the competent authorities responsible for the authorisation and prudential supervision of payment institutions which are to carry out the duties provided for under Title II either public authorities, or bodies recognised by national law or by public authorities expressly empowered for that purpose

²⁷³ Outsourcing of important operational functions may not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authorities to monitor the payment institution's compliance with all obligations laid down in this Directive.

by national law, including national central banks. The competent authorities must guarantee independence from economic bodies and avoid conflicts of interest.²⁷⁴

Article 20(3)3 requires that where there is more than one competent authority for matters covered by Title II in each territory, Member States must ensure that those authorities cooperate closely so that they can discharge their respective duties effectively. The same applies in cases where the authorities competent for matters covered by Title II are not the competent authorities responsible for the supervision of credit institutions.

3.2.2.5.14 *Supervision*

Member States are required, as set out in Article 21 to ensure that the controls exercised by the competent authorities for checking continued compliance with Title II are proportionate, adequate and responsive to the risks to which payment institutions are exposed. In order to check compliance with Title II, the competent authorities shall be entitled to take the following steps, in particular:

- to require the payment institution to provide any information needed to monitor compliance;
- to carry out on-site inspections at the payment institution, at any agent or branch providing payment services under the responsibility of the payment institution, or at any entity to which activities are outsourced;
- to issue recommendations, guidelines and, if applicable, binding administrative provisions; and
- to suspend or withdraw authorisation in cases referred to in Article 12.

Without prejudice to the procedures for the withdrawal of authorisations and the provisions of criminal law, Member States are required to provide that their respective competent authorities, may, as against payment institutions or those who effectively control the business of payment institutions which breach laws, regulations or administrative provisions concerning the supervision or pursuit of their payment service business, adopt or impose in respect of them penalties or measures aimed specifically at ending observed breaches or the causes of such breaches.

3.2.2.5.15 *Professional Secrecy*

Article 22 requires that Member States ensure that all persons working or who have worked for the competent authorities, as well as experts acting on behalf of the competent authorities, are bound by the obligation of professional secrecy, without prejudice to cases covered by criminal law.²⁷⁵

²⁷⁴ Payment institutions, credit institutions, electronic money institutions, or post office giro institutions may not be designated as competent authorities.

²⁷⁵ In the exchange of information in accordance with Article 24, professional secrecy must be strictly applied to ensure the protection of individual and business rights. Member States may apply this Article taking into account, mutatis mutandis, Articles 44 to 52 of Directive 2006/48/EC.

3.2.2.5.16 *Right to Apply to the Courts*

Member States must ensure that in compliance with Article 23 that decisions taken by the competent authorities in respect of a payment institution pursuant to the laws, regulations and administrative provisions adopted in accordance with the PSD may be contested before the courts. This also applies in respect of a failure to act.

3.2.2.5.17 *Exchange of information*

Article 24 requires the competent authorities of the different Member States to cooperate with each other and, where appropriate, with the European Central Bank and the national central banks of the Member States and other relevant competent authorities designated under Community or national legislation applicable to payment service providers. In addition, Member States must allow the exchange of information between their competent authorities and the following:

- the competent authorities of other Member States responsible for the authorisation and supervision of payment institutions;
- the European Central Bank and the national central banks of Member States, in their capacity as monetary and oversight authorities, and, where appropriate, other public authorities responsible for overseeing payment and settlement systems;
- other relevant authorities designated under this Directive, Directive 95/46/EC, Directive 2005/60/EC and other Community legislation applicable to payment service providers, such as legislation applicable to the protection of individuals with regard to the processing of personal data as well as money laundering and terrorist financing.

3.2.2.5.18 *Exercise of the Right of Establishment and Freedom to Provide Services*

In terms of Article 25, any authorised payment institution that wants to provide payment services for the first time in a Member State other than its home Member State, in exercise of the right of establishment or the freedom to provide services, is required to inform the competent authorities in its home Member State. Within one month of receiving that information, the competent authorities of the home Member State must inform the competent authorities of the host Member State of the name and address of the payment institution, the names of those responsible for the management of the branch, its organisational structure and of the kind of payment services it intends to provide in the territory of the host Member State. Competent authorities are also required to provide each other with all essential and/or relevant information. This includes infringements or suspected infringements by an agent, a branch or an entity to which activities are outsourced.

3.2.2.5.19 *Waiver*

Article 26(1) permits Member States to waive or allow their competent authorities to waive the application of all or part of the procedure and conditions set out in Section 1 (General Rules), Section 2 (Other Requirements) and Section 3 (Competent Authorities and Supervision) with the exception of Articles 20 (Designation of Competent Authorities), 22 (professional secrecy), 23 (right to apply to the courts) and 24 (exchange of information) and allow natural or legal persons to be entered in the register provided for in Article 13, where:

- The average of the preceding 12 months' total amount of payment transactions executed by the person concerned, including any agent for which it assumes full responsibility, does not exceed EUR 3 million per month. That requirement shall be assessed on the projected total amount of payment transactions in its business plan, unless an adjustment to that plan is required by the competent authorities (Article 26(1)(a)); and
- None of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes (Article 26(1)(b)).

Persons referred to in Article 26(1) must have their head office or place of residence in the Member State in which it actually carries on its business (Article 26(2)). These persons shall be treated as payment institutions, save that Article 10(g) and Article 25 shall not apply to them (Article 26(3)). Member States may also provide that any natural or legal person registered in accordance with Article 26(1) may engage only in certain activities listed in Article 16 (Article 26(4)).²⁷⁶

3.2.2.5.20 Notification and Information (Waiver)

If a Member State avails itself of the waiver provided for in Article 26, it was required to notify the Commission accordingly by 1 November 2009 and to notify the Commission forthwith of any subsequent change. In addition, the Member State are required to inform the Commission of the number of natural and legal persons concerned and, on an annual basis, of the total amount of payment transactions executed as of 31 December of each calendar year, as referred to in Article 26(1)(a).

3.2.2.5.21 Access to Payment Systems

Article 28 covers access to payment systems. In terms of Article 28(1), Member States are required to ensure that the rules on access of authorised or registered payment service providers that are legal persons to payment systems are **objective, non-discriminatory and proportionate** and that those rules do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system.

Payment systems shall impose on payment service providers, on payment service users or on other payment systems none of the following requirements:

- any restrictive rule on effective participation in other payment systems;
- any rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; or
- any restriction on the basis of institutional status.

Article 28(1) does not however apply to:

²⁷⁶ Article 26(5) requires the persons referred to in Article 26(1) to notify the competent authorities of any change in their situation which is relevant to the conditions specified in that paragraph. Member States must take the necessary steps to ensure that where the conditions set out in paragraphs 1, 2 and 4 are no longer fulfilled, the persons concerned shall seek authorisation within 30 calendar days in accordance with the procedure laid down in Article 10.

- payment systems designated under Directive 98/26/EC (designated payment and securities settlement systems);
- payment systems composed exclusively of payment service providers belonging to a group composed of entities linked by capital where one of the linked entities enjoys effective control over the other linked entities; or
- payment systems where a sole payment service provider (whether as a single entity or as a group):
 - acts or can act as the payment service provider for both the payer and the payee and is exclusively responsible for the management of the system, and
 - licenses other payment service providers to participate in the system and the latter have no right to negotiate fees between or amongst themselves in relation to the payment system although they may establish their own pricing in relation to payers and payees.

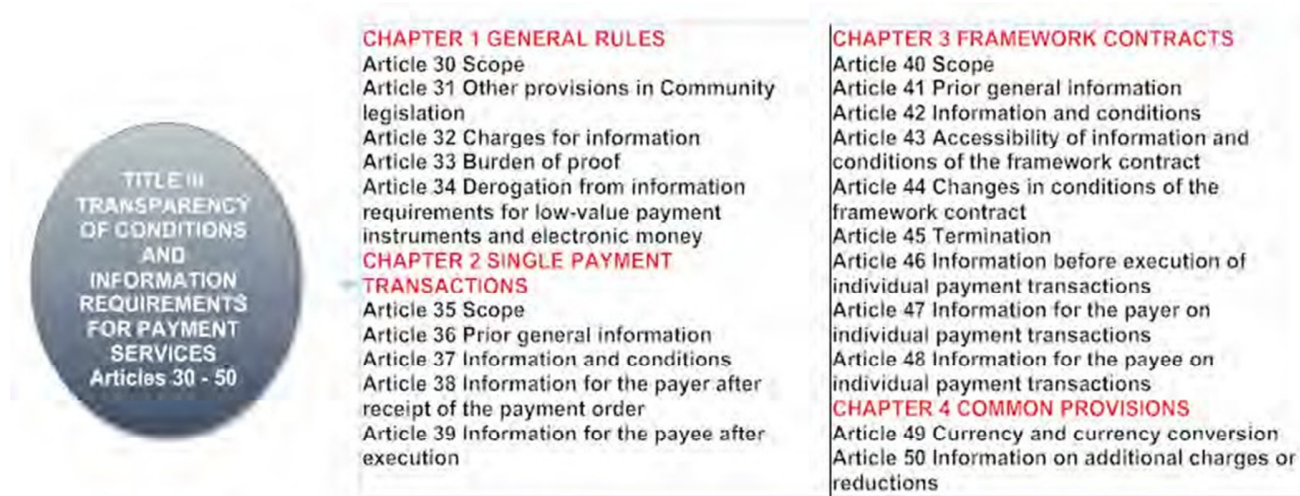
3.2.2.5.22 *Prohibition for Persons other than Payment Service Providers to Provide Payment Services*

Article 29 explicitly prohibits natural or legal persons that are neither payment service providers nor explicitly excluded from the scope of this Directive from providing the payment services listed in the Annex.

TITLE III TRANSPARENCY OF CONDITIONS AND INFORMATION REQUIREMENTS FOR PAYMENT SERVICES

Title II of the PSD covers the transparency of conditions and information requirements for payment services. Title II is divided into four chapters, namely, Chapter 1) General Rules, Chapter 2) Single Payment Transactions, Chapter 3) Framework Contracts; and Chapter 4) Common Provisions. Title III therefore applies to single payment transactions, framework contracts and payment transactions covered by them. The individual Articles under each chapter are schematically presented in Diagram 6 below.

Diagram 6: Content of Title III



3.2.2.5.23 *Charges for Information*

Article 32(1) expressly prohibits payment service providers from charging the payment service users for providing information under Title III. However, as per Article 32(2), the payment service provider and the payment service user are permitted to agree on charges for additional or more frequent information, or transmission by means of communication other than those specified in the framework contract, provided at the payment service user's request.²⁷⁷

3.2.2.5.24 *Burden of Proof on Information Requirements*

Member States are permitted in terms of Article 33 to stipulate that the burden of proof shall lie with the payment service provider to prove that it has complied with the information requirements set out in Title III.

3.2.2.5.25 *Derogation from Information Requirements for Low-value Payment Instruments and Electronic Money*

Article 34 provides an exemption (derogation) from several of the information requirements in the PSD. As per Article 34(1), in cases of payment instruments which, according to the framework contract, concern only **individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time:**

- (a) by way of derogation from Articles 41, 42 and 46, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed to

²⁷⁷ These charges for additional or more frequent information must be appropriate and in line with the payment service provider's actual costs.

take an informed decision as well as an indication of where any other information and conditions specified in Article 42 are made available in an easily accessible manner;

- (b) it may be agreed that, by way of derogation from Article 44, the payment service provider will not be required to propose changes in the conditions of the framework contract in the same way as provided for in Article 41(1);
- (c) it may be agreed that, by way of derogation from Articles 47 and 48, after the execution of a payment transaction:
 - (i) the payment service provider shall provide or make available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges and/ or, in the case of several payment transactions of the same kind made to the same payee, information on the total amount and charges for those payment transactions;
 - (ii) the payment service provider is not required to provide or make available information referred to in point (i) if the payment instrument is used **anonymously** or if the payment service provider is not otherwise technically in a position to provide it. However, the payment service provider is required to provide the payer with a possibility to verify the amount of funds stored.

Article 34(2) states that for national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in Article 34(1) and for prepaid payment instruments, Member States may increase those amounts up to EUR 500.

3.2.2.5.26 *Single Payment Transaction – Prior General Information*

Chapter 2 of Title III covers single payment transactions. Article 36(1) requires Member States to require that before the payment service user is bound by any single payment service contract or offer, the payment service provider, in an easily accessible manner, makes available to the payment service user the information and conditions specified in Article 37. At the payment service user's request, the payment service provider must provide the information and conditions on paper or on another durable medium. The information and conditions must be given in easily understandable words and in a clear and comprehensible form, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.²⁷⁸

3.2.2.5.27 *Single Payment Transaction - Information and Conditions*

In fulfilment of the obligations set out in Article 37(1), Member States must ensure that the following information and conditions are provided or made available to the payment service user:

²⁷⁸ Article 36(2) states that if the single payment service contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with Article 36(1), the payment service provider must fulfil its obligations under that paragraph immediately after the execution of the payment transaction.

- a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly executed (Article 37(1)(a));
- the maximum execution time for the payment service to be provided (Article 37(1)(b));
- all charges payable by the payment service user to his payment service provider and, where applicable, the breakdown of the amounts of any charges (Article 37(1)(c));
- where applicable, the actual or reference exchange rate to be applied to the payment transaction (Article 37(1)(d)).

3.2.2.5.28 *Single Payment Transaction - Information for the Payer after Receipt of the Payment Order*

Article 38 requires the payer's payment service provider, immediately after receipt of the payment order, to provide or make available to the payer, in the same way as provided for in Article 36(1), the following information:

- a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee (Article 38(1)(a));
- the amount of the payment transaction in the currency used in the payment order (Article 38(1)(b));
- the amount of any charges for the payment transaction payable by the payer and, where applicable, a breakdown of the amounts of such charges (Article 38(1)(c));
- where applicable, the exchange rate used in the payment transaction by the payer's payment service provider or a reference thereto, when different from the rate provided in accordance with Article 37(1)(d), and the amount of the payment transaction after that currency conversion (Article 38(1)(d)); and
- the date of receipt of the payment order (Article 38(1)(e)).

3.2.2.5.29 *Single Payment Transaction - Information for the Payee After Execution*

In addition to the information that must be provided to the payer by the payer's payment service provider, Article 39 lists the information that must be provided to the payee by the payee's payment service provider immediately after the execution of the payment transaction. The following information must be provided:

- the reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction (Article 39(a));
- the amount of the payment transaction in the currency in which the funds are at the payee's disposal (Article 39(b));
- the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amount of such charges (Article 39(c));
- where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion (Article 39(d)); and
- the credit value date (Article 39(e)).

3.2.2.5.30 *Framework Contracts - Prior General Information*

Chapter 3 of Title III covers the information requirements for framework contracts. Article 41(1) requires Member States to require that, in good time before the payment service user is bound by any framework

contract or offer, the payment service provider provide the payment service user on paper or on another durable medium with the information and conditions specified in Article 42. The information and conditions must be given in easily understandable words and in a clear and comprehensible form, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.²⁷⁹

3.2.2.5.31 Framework Contracts - Information and Conditions

Article 42 sets out the information and conditions the must be provided to the payment service user. These are set out in Table 19 below.

Table 19: Information that must be provided prior to Entering into a Framework Contract or Offer

Information category	Article	Information required
Payment service provider	42(1)(a)	The name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in the Member State where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider
	42(1)(b)	The particulars of the relevant supervisory authorities and of the register provided for in Article 13 or of any other relevant public register of authorisation of the payment service provider and the registration number, or equivalent means of identification in that register.
Use of the payment service	42(2)(a)	A description of the main characteristics of the payment service to be provided.
	42(2)(b)	A specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly executed.
	42(2)(c)	The form of and procedure for giving consent to execute a payment transaction and withdrawal of such consent in accordance with Articles 54 and 66.
	42(2)(d)	A reference to the point in time of receipt of a payment order as defined in Article 64 and the cut-off time, if any, established by the payment service provider.
	42(2)(e)	The maximum execution time for the payment services to be provided.
	42(2)(f)	Whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Article 55(1).
Charges, interest & exchange rates	42(3)(a)	All charges payable by the payment service user to the payment service provider and, where applicable, the breakdown of the amounts of any charges.
	42(3)(b)	Where applicable, the interest and exchange rates to be applied or, if

²⁷⁹ In terms of Article 42(2), if the framework contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with Article 42(1), the payment service provider must fulfil its obligations under that paragraph immediately after the conclusion of the frameworkcontract.

		reference interest and exchange rates are to be used, the method of calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate.
	42(3)(c)	If agreed, the immediate application of changes in reference interest or exchange rate and information requirements related to the changes in accordance with Article 44(2).
Communication	42(4)(a)	Where applicable, the means of communication, including the technical requirements for the payment service user's equipment, agreed between the parties for the transmission of information or notifications under this Directive.
	42(4)(b)	The manner in and frequency with which information under this Directive is to be provided or made available.
	42(4)(c)	The language or languages in which the framework contract will be concluded and communication during this contractual relationship undertaken.
	42(4)(d)	The payment service user's right to receive the contractual terms of the framework contract and information and conditions in accordance with Article 43.
Safeguards & Corrective Measures	42(5)(a)	Where applicable, a description of steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for the purposes of Article 56(1)(b).
	42(5)(b)	If agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Article 55.
	42(5)(c)	The liability of the payer in accordance with Article 61, including information on the relevant amount.
	42(5)(d)	How and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly executed payment transaction in accordance with Article 58 as well as the payment service provider's liability for unauthorised payment transactions in accordance with Article 60.
	42(5)(e)	The liability of the payment service provider for the execution of payment transactions in accordance with Article 75.
	42(5)(f)	The conditions for refund in accordance with Articles 62 and 63.
Changes in and termination of framework contract	42(6)(a)	If agreed, information that the payment service user will be deemed to have accepted changes in the conditions in accordance with Article 44, unless he notifies the payment service provider that he does not accept them before the date of their proposed date of entry into force.
	42(6)(b)	The duration of the contract.
	42(6)(c)	The right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with Article 44(1) and Article 45.
Redress	42(7)(a)	Any contractual clause on the law applicable to the framework contract and/or the competent courts.
	42(7)(b)	The out-of-court complaint and redress procedures available to the payment service user in accordance with Articles 80 to 83.

3.2.2.5.32 Framework Contracts - Accessibility of Information and Conditions of the Framework Contract

At any time during the contractual relationship the payment service user must, as required by Article 43, have a right to receive, on request, the contractual terms of the framework contract as well as the information and conditions specified in Article 42 on paper or on another durable medium.

3.2.2.5.33 Framework Contracts - Changes in Conditions of the Framework Contract

Any changes in the framework contract as well as the information and conditions specified in Article 42, must be proposed by the payment service provider in the same way as provided for in Article 41(1) and no later than two months before their proposed date of application. However, as per Article 44(2), changes in the interest or exchange rates may be applied immediately and without notice, provided that such a right is agreed upon in the framework contract and that the changes are based on the reference interest or exchange rates agreed on in accordance with Article 42(3)(b) and (c).²⁸⁰

3.2.2.5.34 Framework Contracts – Termination

Article 45 specifies the conditions for termination. Article 45(1) states that, the payment service user may terminate the framework contract at any time, unless the parties have agreed on a period of notice. Such a period may not exceed one month. The termination of a framework contract concluded for a fixed period exceeding 12 months or for an indefinite period must be free of charge for the payment service user after the expiry of 12 months. In all other cases charges for the termination must be appropriate and in line with costs. In terms of Article 45(3), if agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an indefinite period by giving at least two months' notice in the same way as provided for in Article 41(1). Charges for payment services levied on a regular basis are payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, they must be reimbursed proportionally Article 45(4).²⁸¹

3.2.2.5.35 Framework Contracts - Information Before Execution of Individual Payment Transactions

Article 46 deals with the situation where an individual payment transaction under a framework contract is initiated by the payer. In this circumstance a payment service provider is required, at the payer's request for this specific payment transaction, to provide explicit information on the maximum execution time and the charges payable by the payer and, where applicable, a breakdown of the amounts of any charges.

²⁸⁰ Article 44(3) requires that changes in the interest or exchange rate used in payment transactions must be implemented and calculated in a neutral manner that does not discriminate against payment service users.

²⁸¹ The provisions of this Article are without prejudice to the Member States' laws and regulations governing the rights of the parties to declare the framework contract unenforceable or void.

3.2.2.5.36 Framework Contracts - Information for the Payer on Individual Payment Transactions

As per Article 47(1), after the amount of an individual payment transaction is debited from the payer's account or, where the payer does not use a payment account, after the receipt of the payment order, the payer's payment service provider is required to provide the payer without undue delay with the following information:

- a reference enabling the payer to identify each payment transaction and, where appropriate, information relating to the payee Article (47(1)(a));
- the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order (Article 47(1)(b));
- the amount of any charges for the payment transaction and, where applicable, a breakdown thereof, or the interest payable by the payer (Article 47(1)(c));
- where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion (Article 47(1)(d));
- the debit value date or the date of receipt of the payment order (Article 47(1)(e)).

3.2.2.5.37 Framework Contracts - Information for the Payee on Individual Payment Transactions

Article 48(1) sets out the information that the payee's payment service provider must provide the payee after the execution of an individual payment transaction as follows:

- the reference enabling the payee to identify the payment transaction and, where appropriate, the payer, and any information transferred with the payment transaction (Article 48(1)(a));
- the amount of the payment transaction in the currency in which the payee's payment account is credited (Article 48(1)(b));
- the amount of any charges for the payment transaction and, where applicable, a breakdown thereof, or the interest payable by the payee (Article 48(1)(d));
- where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion (Article 48(1)(e)); and
- the credit value date (Article 48(1)(f)).

Article 48(2) permits a framework contract to include a condition that the information referred to in Article 48(1) is to be provided or made available periodically at least once a month and in an agreed manner which allows the payee to store and reproduce information unchanged.

3.2.2.5.38 Common Provisions - Currency and Currency Conversion

The first common provision under Title III deals with currency and currency conversion. In terms of Article 49(1), payments must be made in the currency agreed between the parties. Where a currency conversion service is

offered prior to the initiation of the payment transaction and where that currency conversion service is offered at the point of sale or by the payee, the party offering the currency conversion service to the payer is required to disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction (Article 49(2)).

3.2.2.5.39 *Common Provisions - Information on Additional Charges or Reductions*

Article 50(1) requires that where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee is required to inform the payer thereof prior to the initiation of the payment transaction. In terms of Article 50(2), where, for the use of a given payment instrument, a payment service provider or a third party requests a charge, he is required to inform the payment service user thereof prior to the initiation of the payment transaction.

TITLE IV RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES (PAYMENT INSTRUMENTS)

Title IV covers the rights and obligations in relation to the provision and use of payment services. This title is divided into five chapters as follows: Chapter 1) Common Provisions; Chapter 2) Authorisation of Payment Transactions; Chapter 3) Execution of Payment Transactions; Chapter 4) Data Protection and Chapter 5) Out of Court Complaint and Redress Procedures for the Settlement of Disputes. The individual Articles under each chapter are schematically presented in Diagram 7 below.

Diagram 7: Content of Title IV



3.2.2.5.40 Charges Applicable

Article 52 prohibits the payment service provider from charging the payment service user for fulfilment of its information obligations or corrective and preventive measures under Title IV, unless otherwise specified in Articles 65(1), 66(5) and 74(2). Those charges must be agreed between the payment service user and the payment service provider and must be appropriate and in line with the payment service provider's actual costs.

Where a payment transaction does not involve any currency conversion, Member States must require, in terms of Article 52(2) that the payee pays the charges levied by his payment service provider, and the payer pays the charges levied by his payment service provider.

In terms of Article 52(3), the payment service provider must not prevent the payee from requesting from the payer a charge or from offering him a reduction for the use of a given payment instrument. However, Member States may forbid or limit the right to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments.

3.2.2.5.41 Derogation for Low Value Payment Instruments and Electronic Money

Article 53(1) provides that in the case of payment instruments which according to the framework contract, solely concern **individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150 or store funds which do not exceed EUR 150** at any time payment service providers may agree with their payment service users that:

- Article 56(1)(b)²⁸² and Article 57(1)(c)²⁸³ and (d)²⁸⁴ as well as Article 61(4)²⁸⁵ and (5)²⁸⁶ do not apply if the payment instrument does not allow its blocking or prevention of its further use (Article 53(1)(a));
- Articles 59, 60 and Article 61(1) and (2) do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised (Article 53(1)(b));
- by way of derogation from Article 65(1), the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context (Article 53(1)(c));
- by way of derogation from Article 66, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee (Article 51(1)(d));
- by way of derogation from Articles 69 and 70, other execution periods apply (Article 51(1)(e)).

As per Article 51(2), for national payment transactions, Member States or their competent authorities are permitted to reduce or double the amounts referred to in Article 53(1). They may increase them for prepaid payment instruments up to EUR 500.

3.2.2.5.42 *Authorisation of Payment Transactions – Consent and Withdrawal of Consent*

Article 54(1) requires Member States to ensure that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and his payment service provider, after the execution of the payment transaction. Consent to execute a payment transaction or a series of payment transactions will be given in the form agreed between the payer and his payment service provider (Article 54(2)).²⁸⁷

²⁸² Article 56(1)(b) reads, “the payment service user entitled to use a payment instrument shall have the following obligations: to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use.”

²⁸³ Article 57(1)(c) reads, “the payment service provider issuing a payment instrument shall have the following obligations: to ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 56(1)(b) or request unblocking pursuant to Article 55(4); on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that he made such notification.”

²⁸⁴ Article 57(1)(d) reads, “the payment service provider issuing a payment instrument shall have the following obligations: to prevent all use of the payment instrument once notification pursuant to Article 56(1)(b) has been made.”

²⁸⁵ Article 61(4) reads, “the payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with Article 56(1)(b), except where he has acted fraudulently.”

²⁸⁶ Article 61(5) reads, “if the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under Article 57(1)(c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where he has acted fraudulently.”

²⁸⁷ In the absence of such consent, a payment transaction shall be considered to be unauthorised.

Article 54(3) states that consent may be withdrawn by the payer at any time, but no later than the point in time of irrevocability under Article 66. Consent to execute a series of payment transactions may also be withdrawn with the effect that any future payment transaction is to be considered as unauthorised.²⁸⁸

3.2.2.5.43 Authorisation of Payment Transactions – Limits of the Use of the Payment Instrument

In cases where a specific payment instrument is used for the purposes of giving consent, Article 55(1) provides that the payer and his payment service provider may agree on spending limits for payment transactions executed through that payment instrument.

Article 55(2) provides further that if agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons related to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil his liability to pay. In such cases, Article 55(3) requires the payment service provider to inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible, before the payment instrument is blocked and at the latest immediately thereafter, unless giving such information would compromise objectively justified security reasons or is prohibited by other relevant Community or national legislation. The payment service provider may unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist (Article 55(4)).

3.2.2.5.44 Obligations of the Payment Service User in Relation to Payment Instruments

Article 56 sets out the obligations of the payment service user in relation to payment instruments and states that a payment service user entitled to use a payment instrument has the following obligations:

- to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument (Article 56(1)(a))²⁸⁹; and
- to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use (Article 56(1)(b)).

3.2.2.5.45 Obligations of the Payment Service Provider in Relation to Payment Instruments

Article 57 sets out the obligations of payment services providers in relation to the issuing of payment instruments as follows:

- to make sure that the personalised security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 56 (Article 57(1)(a));

²⁸⁸ The procedure for giving consent must be agreed between the payer and the payment service provider.

²⁸⁹ The payment service user is required, as soon as he receives a payment instrument, to take all reasonable steps to keep its personalised security features safe.

- to refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced (Article 57(1)(b));
- to ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 56(1)(b) or request unblocking pursuant to Article 55(4); on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that he made such notification (Article 57(1)(c)); and
- to prevent all use of the payment instrument once notification pursuant to Article 56(1)(b) has been made (Article 57(1)(e)).

The payment service provider bears the risk of sending a payment instrument to the payer or of sending any personalised security features of it (Article 57(2)).

3.2.2.5.46 Notification of Unauthorised or Incorrectly Executed Payment Transactions

In terms of Article 58, the payment service user will obtain rectification from the payment service provider only if he notifies his payment service provider without undue delay on becoming aware of any unauthorised or incorrectly executed payment transactions giving rise to a claim, including that under Article 75, and no later than 13 months after the debit date, unless, where applicable, the payment service provider has failed to provide or make available the information on that payment transaction in accordance with Title III.

3.2.2.5.47 Evidence on Authentication and Execution of Payment Transactions

Article 59(1) requires Member States to require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.²⁹⁰

3.2.2.5.48 Payment Service Provider's Liability for Unauthorised Payment Transactions

Article 60(1) states that Member States are required to ensure that, without prejudice to Article 58, in the case of an unauthorised payment transaction, the payer's payment service provider refunds to the payer immediately the amount of the unauthorised payment transaction and, where applicable, restores the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.²⁹¹

²⁹⁰ As per Article 59(2), where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.

²⁹¹ Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and his payment service provider.

3.2.2.5.49 *Payer's Liability for Unauthorised Payment Transactions*

Article 61(1), by way of derogation of Article 60, states that the payer will bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment instrument or, if the payer has failed to keep the personalised security features safe, from the misappropriation of a payment instrument.

In addition, the payer will, in terms of Article 61(2), bear all the losses relating to any unauthorised payment transactions if he incurred them by acting fraudulently or by failing to fulfil one or more of his obligations under Article 56 with intent or gross negligence. In such cases, the maximum amount referred to in of this Article 61(1) shall not apply.

However, in cases where the payer has neither acted fraudulently nor with intent failed to fulfil his obligations under Article 56, Member States may reduce the liability referred to in Article 61(1) and Article 61(2), taking into account, in particular, the nature of the personalised security features of the payment instrument and the circumstances under which it was lost, stolen or misappropriated.

In terms of Article 61(4), the payer will not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with Article 56(1)(b), except where he has acted fraudulently. It must be noted however that in terms of Article 61(5), if the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under Article 57(1)(c), the payer will not be liable for the financial consequences resulting from use of that payment instrument, except where he has acted fraudulently.

3.2.2.5.50 *Refunds for Payment Transactions Initiated by or Through a Payee*

Article 62 requires Member States to ensure that a payer is entitled to a refund from his payment service provider of an authorised payment transaction initiated by or through a payee which has already been executed, if the following conditions are met:

- the authorisation did not specify the exact amount of the payment transaction when the authorisation was made (Article 62(1)(a)); and
- the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account his previous spending pattern, the conditions in his framework contract and relevant circumstances of the case (Article 62(1)(b)).²⁹²

²⁹² In terms of Article 62(3), it may be agreed in the framework contract between the payer and the payment service provider that the payer has no right to a refund where he has given his consent to execute the payment transaction directly to his payment service provider and, where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least four weeks before the due date by the payment service provider or by the payee.

3.2.2.5.51 *Requests for Refunds for Payment Transactions Initiated by or Through a Payee*

Member States must in terms of Article 63(1), ensure that the payer can request the refund referred to in Article 62 of an authorised payment transaction initiated by or through a payee for a period of eight weeks from the date on which the funds were debited. Article 63(2) requires that within ten business days of receiving a request for a refund, the payment service provider shall either refund the full amount of the payment transaction or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter in accordance with Articles 80 to 83 if he does not accept the justification provided.

3.2.2.5.52 *Payment Orders and Amounts Transferred – Receipt of Payment Orders*

Article 64(1) requires Member States to ensure that the point in time of receipt is the time when the payment order transmitted directly by the payer or indirectly by or through a payee is received by the payer's payment service provider. If the point in time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.

However, if the payment service user initiating a payment order and his payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has set funds at his payment service provider's disposal, the point in time of receipt for the purposes of Article 69 is deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day (Article 64(2)).

3.2.2.5.53 *Refusal of Payment Orders*

In terms of Article 65(1), where the payment service provider refuses to execute a payment order, the refusal and, if possible, the reasons for it and the procedure for correcting any factual mistakes that led to the refusal must be notified to the payment service user, unless prohibited by other relevant Community or national legislation. The payment service provider is required to provide or make available the notification in an agreed manner at the earliest opportunity, and in any case, within the periods specified in Article 69.²⁹³

3.2.2.5.54 *Irrevocability of a Payment Order By a Payment Service User*

Article 66(1) requires Member States to ensure that the payment service user may not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in Article 66. Where the payment transaction is initiated by or through the payee, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee (Article 66(2)).²⁹⁴

²⁹³ The framework contract may include a condition that the payment service provider may charge for such a notification if the refusal is objectively justified.

²⁹⁴ The payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.

However, in the case of a direct debit and without prejudice to refund rights the payer may revoke the payment order at the latest by the end of the business day proceeding the day agreed for debiting the funds (Article 66(3)).

After the time limits specified above, the payment order may be revoked only if agreed between the payment service user and his payment service provider.

3.2.2.5.55 *Amounts Transferred and Amounts Received*

In terms of Article 67(1), Member States must require the payment service provider of the payer, the payment service provider of the payee and any intermediaries of the payment service providers to **transfer the full amount of the payment transaction** and refrain from deducting charges from the amount transferred.

However, in terms of Article 67(2), the payee and his payment service provider may agree that the payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges must be separated in the information given to the payee.²⁹⁵

3.2.2.5.56 *Execution Time and Value Date*

Section 2 of Title IV applies to payment transactions in euro; national payment transactions in the currency of the Member State outside the euro area concerned; and payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro.²⁹⁶

3.2.2.5.57 *Payment Transactions to a Payment Account*

Member States must, in terms of Article 69, require the payer's payment service provider to ensure that, after the point in time of receipt in accordance with Article 64, the amount of the payment transaction is credited to the payee's payment service provider's account at the latest by the end of the next business day.²⁹⁷

Member States must also require the payment service provider of the payee to value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with Article 73 and require the payee's payment service provider to transmit a

²⁹⁵ If any charges other than those referred to in Article 67(2) are deducted from the amount transferred, the payment service provider of the payer must ensure that the payee receives the full amount of the payment transaction initiated by the payer. In cases where the payment transaction is initiated by or through the payee, his payment service provider must ensure that the full amount of the payment transaction is received by the payee.

²⁹⁶ This Section also applies to other payment transactions, unless otherwise agreed between the payment service user and his payment service provider, with the exception of Article 73, which is not at the disposal of the parties. However, when the payment service user and his payment service provider agree on a longer period than those laid down in Article 69, for intra-Community payment transactions such period shall not exceed 4 business days following the point in time of receipt in accordance with Article 64.

²⁹⁷ Until 1 January 2012, a payer and his payment service provider were permitted to agree on a period no longer than three business days. These periods could be extended by a further business day for paper initiated payment transactions.

payment order initiated by or through the payee to the payer's payment service provider within the time limits agreed between the payee and his payment service provider, enabling settlement, as far as direct debit is concerned, on the agreed due date.

3.2.2.5.58 *Absence of Payee's Payment Account with the Payment Service Provider*

In the case where the payee does not have a payment account with the payment service provider, the funds must be made available to the payee by the payment service provider who receives the funds for the payee within the period specified in Article 69 (Article 70).

3.2.2.5.59 *Cash Placed on a Payment Account*

Article 71 requires that where a consumer places cash on a payment account with that payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after the point of time of the receipt of the funds. Where the payment service user is not a consumer, the amount must be made available and value dated at the latest on the next business day after the receipt of the funds.

3.2.2.5.60 *National Payment Transactions*

For national payment transactions, Member States may provide for shorter execution times (Article 72).

3.2.2.5.61 *Value Date and Availability of Funds*

Article 73(1) requires Member States to ensure that the credit value date for the payee's payment account is no later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account. The payment service provider of the payee must ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account.

Additionally, Article 73(2) requires Member States to ensure that the debit value date for the payer's payment account is no earlier than the point in time at which the amount of the payment transaction is debited to that payment account.

3.2.2.5.62 *Liability - Incorrect Unique Identifiers*

In terms of Article 74(1), if a payment order is executed in accordance with the unique identifier, the payment order is deemed to have been executed correctly with regard to the payee specified by the unique identifier. However, if the unique identifier provided by the payment service user is incorrect, the payment service provider will not be liable under Article 75 for non-execution or defective execution of the payment transaction. The payer's payment service provider is however required to make reasonable efforts to recover the funds involved in the payment transaction. Additionally, if agreed in the framework contract, the payment service provider may charge the payment service user for recovery.

3.2.2.5.63 *Liability - Non-execution or Defective Execution*

Where a payment order is initiated by the payer, Article 75(1) states that his payment service provider is, without prejudice to Article 58, Article 74 (2) and (3), and Article 78, liable to the payer for correct execution of the payment transaction, unless he can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 69 (1), in which case, the payee's payment service provider is liable to the payee for the correct execution of the payment transaction.²⁹⁸

Where a payment order is initiated by or through the payee, Article 75(2) states that his payment service provider is, without prejudice to Article 58, Article 74(2) and (3), and Article 78, liable to the payee for correct transmission of the payment order to the 5.12.2007 EN Official Journal of the European Union L 319/31 payment service provider of the payer in accordance with Article 69(3).²⁹⁹ In addition, the payment service provider of the payee is, without prejudice to Article 58, Article 74(2) and (3), and Article 78, liable to the payee for handling the payment transaction in accordance with its obligations under Article 73.³⁰⁰

3.2.2.5.64 *Right of Recourse*

As per Article 77(1), where the liability of a payment service provider under Article 75 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary is required to compensate the first payment service provider for any losses incurred or sums paid under Article 75.³⁰¹

3.2.2.5.65 *Data Protection*

Data protection requirements are provided for in Article 79. This article states that Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of such personal data shall be carried out in accordance with Directive 95/46/EC.

²⁹⁸ Where the payer's payment service provider is liable under Article 75(1), he shall without undue delay refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place. Where the payee's payment service provider is liable under the Article 75(1), he shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account.

In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by the payer, his payment service provider shall regardless of liability under this paragraph, on request, make immediate efforts to trace the payment transaction and notify the payer of the outcome.

²⁹⁹ Where the payee's payment service provider is liable under this subparagraph, he is required to immediately re-transmit the payment order in question to the payment service provider of the payer.

³⁰⁰ Where the payee's payment service provider is liable under this subparagraph, he shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account.

³⁰¹ Article 77(2) states that, "further financial compensation may be determined in accordance with agreements between payment service providers and/or intermediaries and the law applicable to the agreement concluded between them."

3.2.2.5.66 *Complaint Procedures*

Chapter 5 of Title IV covers out-of-court complaint and redress procedures for the settlement of disputes. Article 80(1) that deals with the complaints procedure requires Member States to ensure that procedures are set up which allow payment service users and other interested parties, including consumer associations, to submit complaints to the competent authorities with regard to payment service providers' alleged infringements of the provisions of national law implementing the provisions of the PSD. As per Article 80(2), where appropriate and without prejudice to the right to bring proceedings before a court in accordance with national procedural law, the reply from the competent authorities must inform the complainant of the existence of the out-of-court complaint and redress procedures set up in accordance with Article 83.

3.2.2.5.67 *Penalties*

As required by Article 81(1), Member States must lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to the PSD and take all measures necessary to ensure that they are implemented. Such penalties must be effective, proportionate and dissuasive.³⁰²

3.2.2.5.68 *Complaints Procedure to be Administered by Competent Authorities*

Article 82(1) requires Member States to take all the measures necessary to ensure that the complaints procedures and penalties provided for in Articles 80(1) and 81(1) respectively are administered by the authorities empowered to ensure compliance with the provisions of national law adopted pursuant to the requirements laid down.³⁰³

3.2.2.5.69 *Out-of-Court-Redress*

Member States must ensure that adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and their payment service providers are put in place for disputes concerning rights and obligations arising under the PSD Directive, using existing bodies where appropriate (Article 83(1)). In the case of cross-border disputes, Member States are required to make sure that those bodies cooperate actively in resolving them (Article 83(2)).

TITLE V IMPLEMENTING MEASURES AND PAYMENTS COMMITTEE

Title IV contains two articles. Article 84 sets out implementing measures. Article 84 empowers the Commission, in accordance with the regulatory procedure with scrutiny referred to in Article 85(2), to adopt implementing measures designed to amend non-essential elements of this Directive and relating to the following:

³⁰² Article 81(2) required Member States to notify the Commission of the rules referred to in Article 81(1) and of the competent authorities referred to in Article 82 by 1 November 2009 and to notify the Commission without delay of any subsequent amendment affecting them.

³⁰³ In the event of infringement or suspected infringement of the provisions of national law adopted pursuant to Titles III and IV, the competent authorities referred to in Article 82(1) will be those of the home Member State of the payment service provider, except for agents and branches conducted under the right of establishment where the competent authorities shall be those of the host Member State.

- adapting the list of activities in the Annex, in accordance with Articles 2 to 4 and 16;
- changing the definition of micro enterprise within the meaning of Article 4(26) in accordance with an amendment of Recommendation 2003/361/EC;
- updating the amounts specified in Articles 26(1) and 61(1) in order to take account of inflation and significant market developments.

Article 85(1) states that the Commission shall be assisted by a Payments Committee.

TITLE VI FINAL PROVISIONS

Title VI contains several final provisions including Article 86(1) on full harmonisation which states that, “without prejudice to Article 30(2), Article 33, Article 34(2), Article 45(6), Article 47(3), Article 48(3), Article 51(2), Article 52(3), Article 53(2), Article 61(3), and Articles 72 and 88 insofar as this Directive contains harmonised provisions, Member States shall not maintain or introduce provisions other than those laid down in this Directive.” Article 95 covering transposition required all Member States to bring into force the laws, regulations and administrative provisions necessary to comply with the PSD before 1 November 2009.

Diagram 8: Content of Title V



As the Payment Survives Directive must be transposed into domestic law or regulation, Table 20 below is presented as a reference of the laws and or regulations that were adopted and amendments that were made to existing domestic laws and regulations by several EU Member States to meet this obligation. [Annexure R](#) of this report provides a detailed example of how the Payment services Directive was transposed into domestic law and regulation in Gibraltar.

Table 20: Examples of the National Application of the Payment Services Directive

Member State	National Application of E-Money Directive
France	<ul style="list-style-type: none"> • Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie,³⁰⁴

³⁰⁴ Law n° 2008-776 is an act with a large scope; it does not only concern payment services. It enables the government to adopt the legislative provisions necessary for the transposition of Directive 2007/64/EC through the adoption of an ordinance.

	<ul style="list-style-type: none"> • Ordonnance No 2009-866 du 15 Julliet 2009 relative aux conditions régissant la fourniture de services de paiement et portant creation des établissements de paiement;³⁰⁵ • Décret No. 2009-934 du 29 Julliet pris pour l'application de l'ordonnance No. 2009-866 du 15 Julliet 2009 relative aux conditions régissant la fourniture de services de paiement et portant creation des établissements de paiement;³⁰⁶ • Arrêté du 29 Octobre 2009 portant sur la réglementation prudentielle des établissements de paiement;³⁰⁷ • Arrêté du 29 Juilley 2009 relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principaux stipulations devant figurer dans les conventions de compte de depot et les contrats-cades de services de paiement.³⁰⁸
Netherlands	<ul style="list-style-type: none"> • Het voorstel strekt tot implementatie van richtlijn nr. 2007/64/EG van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt en tot wijziging van de richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG, en tot intrekking van Richtlijn 97/5/EG (PbEU L 319) (de richtlijn). Deze richtlijn geeft een volledig geharmoniseerde regeling voor betaaldiensten in de EU;³⁰⁹ • Besluit van 23 oktober 2009 tot wijziging van het Besluit bekostiging financieel toezicht, het Besluit bestuurlijke boetes financiële sector, het Besluit Markttoegang financiële ondernemingen Wft, het Besluit prudentiële regels Wft, het Besluit prudentieel toezicht financiële groepen Wft en het Besluit Gedragstoezicht financiële ondernemingen Wft ter implementatie van richtlijn 2007/64/EG van het Europees Parlement en de Raad van de Europese Unie van 13 November 2007 betreffende

³⁰⁵ Ordinance No 2009-866 of 15 July 2009 is the main act transposing Directive 2007/64/EC. It amends the legislative part of the Monetary and Financial Code.

³⁰⁶ Decree No 2009-934 of 29 July 2009 is secondary legislation. It completes Ordinance No 2009-866 and amends the regulatory part of the Monetary and Financial Code.

³⁰⁷ Order of 29 October 2009 is secondary legislation. It completes the provisions of the articles inserted in the legislative Part of the Monetary and Financial Code.

Order of 29 October 2009 is related to the prudential regulation of payment institutions.

³⁰⁸ Order of 29 July 2009 is secondary legislation. It completes the provisions of the Articles inserted in the legislative Part of the Monetary and Financial Code. Order of 29 July 2009 is related to the relations between providers of payment services and their clients on disclosure obligations of users of payment services and specifying the main terms to be included in the deposit account agreements and framework contracts of payment services.

³⁰⁹ The Royal Decree of 15 October 2009 provides amendments to the law on Financial Supervision, the Civil Code and the Law on money transaction offices and withdrawal of the Law on cross border payments for the implementation of Directive 2007/64/EC of the European Parliament and the Council concerning payment services in the internal market and for adjustment of the Directive 97/7/EC, 2002/65/EC, 2005/60/EC. Through this amendment the Dutch legislation is adjusted to the Financial Services Directive. This Royal Decree enters into force at the same time as Royal Decree 437, on November 1, 2009. If the Gazette in which this law appears is published after November 1, 2009, it shall enter into force on the day after the date of issue of this Gazette.

	<p>betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG;³¹⁰</p> <ul style="list-style-type: none"> • Regeling van de Minister van Financiën van 26 oktober 2009, nr. FM/2009/2460 U, tot wijziging van de Vrijstellingsregeling Wft in verband met de implementatie van de richtlijn 2007/64/EG van het Europees Parlement en de Raad van de Europese Unie van 13 November 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/48/EG, en tot intrekking van Richtlijn 97/5/EG;³¹¹ • Wet van 28 September 2006, houdende regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht);³¹² • Regeling bedrijfsvoering en administratieve organisaties Wet betreffende de geldtransactiekantoren.³¹³
Portugal	<ul style="list-style-type: none"> • Decreto-Lei No. 317/2009. D.R. n.º 211, Série I de 2009-10-30;³¹⁴

³¹⁰ The Decree of 23 October 2009 provides adjustments to the Ministerial Decisions of the Decree on financing financial supervision, the Decree administrative sanctions in the financial sector, the Decree Market access financial undertakings Wft, the Decree prudential rules Wft, the Decree prudential supervision of financial groups Wft and the Decree supervision of the behaviour of financial undertakings Wft for the implementation of Directive 2007/64/EC of the European Parliament and the Council of the EU on 13 November 2007 concerning payment services in the internal market amending the Directive 97/7/EC, 2002/65/EC, 2005/60/EC and withdrawal of Directive 97/5/EC. Through the amendment of the aforementioned Ministerial Decisions and Decrees by this Royal Decree the Dutch legislation is adjusted to the Financial Services Directive. This act came into force on 1 November 2009.

³¹¹ This Decree is adopted for purposes of implementation of Directive 2007/64/EC. The MD 16444 amends the exemption rule of the Wft in order to bring the Dutch legislation into conformity with the Payment Services Directive. This Decree comes into force simultaneously with Royal Decree 436 and Royal Decree 437, on 1 November 2009. If the Gazette in which this law appears is published after November 1, 2009, it shall enter into force on the day after the date of issue of this Gazette. This Decree is created under Article 26 of the Directive. The Dutch legislator used the option to waive the application of all or part of the procedure and conditions set out in Sections 1 to 3 of the Directive.

³¹² Law of 28 September 2006, on the rules of financial markets and the supervision thereon (Law on Financial Supervision).

³¹³ Regulation on occupational and administrative organization Act on Money Transaction Offices.

³¹⁴ (Decree Law n° 317/2009. Official Journal No 211, Series I of 30 October 2009). DL 317/2009 transposed the new EU framework in terms of payment services into national legislation. DL 317/2009 consists of amendments to several pieces of legislation. The main purpose of DL 317/2009 is to approve, in Annex I, the legal framework which governs the taking up of the business of payment institutions and the provision of payment services (—Regime jurídico que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento). Therefore, Annex I to DL 317/2009 is the main instrument of analysis in this assessment. However, other legislation was also amended as a consequence of the transposition of Directive 2007/64/EC (hereinafter referred to as —the Directivell) into the national legal framework. Articles 3 and 4 of DL 317/2009 amend the Legal Framework on Credit Institutions and Finance Companies (—Regime Geral das Instituições de Crédito e Sociedades Financeiras) which was first approved by Decree Law 298/92. Article 5 of DL 317/2009 amends Law n° 25/2008 which sets preventive and repressive measures against money laundering of benefits with illicit origin and against the terrorist financing. Article 6 of DL 317/2009 amends Annex I to Decree Law 156/2005 laying down the obligatory character of the availability of the complaints book to all the suppliers of goods or service providers which are in contact with the public in general. Article 7 of DL 317/2009 amends Decree Law 95/2006 laying down

	<ul style="list-style-type: none"> • Regime Geral das Instituições de Crédito e Sociedades Financeiras (Aprovado pelo Decreto-Lei No. 298/92, de 31 de Dezembro e alterado posteriormente);³¹⁵ • Decreto-Lei No. 42/2002 de 2 de Março;³¹⁶ • Lei Orgânica do Banco de Portugal.³¹⁷
Ireland	<ul style="list-style-type: none"> • European Communities (Payment Services) Regulations 2009;³¹⁸ • Central Bank Act, 1989; • Central Bank Act, 1942; • Central Bank Reform Act, 2010. • European Communities (Electronic money) Regulations, 2002; • European Communities (Markets in Financial Instruments) Regulations, 2007.

the rules applicable to the distance contracts relating to the financial service concluded with the consumers, transposing into the national legislation Directive 2002/65/EC, of the European Parliament and the Council, of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC. Article 8 amends Law 5/2002 laying down the fight against organised, economic and financial crimes. DL 317/2009 entered into force on 1 November 2009. It was promulgated on 16 October 2009 and enacted on 21 October 2009.

³¹⁵ Legal framework on Credit Institutions and Finance Companies approved by Decree Law nº 298/92 (Approved by Decree Law nº 298/92, of 31 December and later amended).

³¹⁶ DL 42/2002 transposed into the national legislation Directive 2000/28/EC of the European Parliament and of the Council of 18 September 2000 amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions. Directive 2000/28/EC included the electronic money institutions as seen in the definition of the credit institutions. DL 42/2002 also transposed into the national legislation Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. DL 42/2002 lays down the legal basis of the electronic money institutions.

³¹⁷ This Organic Law was approved by Law nº 5/98 of 31 January 1998, and was amended by Decree Law nº 118/2001 of 17 April 2001, Decree Law nº 50/2004 of 10 March 2004 and Decree Law nº 39/2007 of 20 February 2007.

³¹⁸ This Statutory Instrument (hereinafter named the —S.III) transposes Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (hereinafter referred to as —the Directivell). The Directive establishes a harmonised legal framework for the provision of payment services in the European Union / European Economic Area. The Directive: (a) establishes who may provide payments services; (b) introduces an authorisation and supervision framework for a new category of payment services provider called a payment institution; (c) establishes transparency and information requirements to ensure that payment service providers give requisite information to payment service users; and (d) sets out the respective rights and obligations of payment service providers and payment service users.

SECTION 4: DOMESTIC LEGAL AND REGULATORY FRAMEWORKS IN SADC

Section 4 of this report sets out the scope and content of a sound legal basis for the regulations and oversight of the National Payment System and provides a high-level gap analysis highlighting legislation (Acts) and regulations that are legally enforceable in each SADC Member State, draft bills and bills that have been drafted but are not legally enforceable, as they have not been tabled in Parliament or assented to and signed. In addition, the review of the National Payment System Act / Payment System Management Act or Bill in each SADC country has shown a certain level of harmonisation in specific groupings of countries. Mauritius, being the only country in the SADC that has elected not to enact a National Payment System / Payment System Management Act is not included in this Diagram. Tanzania is also not included as, although a National Payment System Bill has been drafted, the Bank of Tanzania informed the authors that at this time, they were not at liberty to share the Bill with third parties. Section 4.3 provides a comparative analysis of the scope of each National Payment System Act and or Bill.

4.1 A Sound Legal Basis

Principle 1 of the PFMI's requires that FMIs should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of their activities in all relevant jurisdictions. Paragraph 3.1.2 of the Bank for International Settlements and International Organization of Securities Commissions *Principles for Financial Market Infrastructures (PFMI) 2012* report reads as follows:

"The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions. The legal basis consists of the legal framework and the FMI's rules, procedures, and contracts. The legal framework includes general laws and regulations that govern, among other things, property, contracts, insolvency, corporations, securities, banking, secured interests, and liability. In some cases, the legal framework that governs competition and consumer and investor protection may also be relevant. Laws and regulations specific to an FMI's activities include those governing its authorisation and its regulation, supervision, and oversight; rights and interests in financial instruments; settlement finality; netting; immobilisation and dematerialisation of securities; arrangements for Delivery versus Payment (DvP), Payment versus Payment (PvP), or Delivery versus Delivery (DvD); collateral arrangements (including margin arrangements); default procedures; and the resolution of an FMI."³¹⁹

Broken down further, a country's laws and regulations should, at the minimum provide for the following:

Regulation and Oversight by the Central Bank: The legal framework should provide for the Central Bank's participation in and oversight of the National Payment System. Central Banks must be mandated to perform functions, implement rules and procedures and take necessary steps to establish, conduct, monitor, regulate and oversee payment clearing and settlement systems. As noted by the Bank for International Settlements, "the legal framework for the payment system needs to support the Central Bank's oversight function. Laws or other legal instruments should be developed to: (i) authorise the Central Bank to oversee, and possibly regulate, the payment system, including the operations of global payment systems within their own borders; (ii) ensure that financial institutions and payment systems effectively manage their financial and operational risk; and (iii) require various payment systems and financial institutions to conduct operations consistent with

³¹⁹ Bank for International Settlements and International Organization of Securities Commissions *Principles for Financial Market Infrastructures* 23.

applicable regulations.” These provisions are more often than not found in the National Payment System Act / Payment System Management Act in each SADC country.

Settlement provisions: Settlement provisions should preferably be contained in legislation rather than contract or multilateral agreement or rules. The law should establish settlement finality and payment finality and irrevocability except under specified conditions. These laws must protect the risk-free settlement facility at the Central Bank from being frozen or attached by creditors of institutions holding settlement accounts. In thirteen of the fourteen SADC countries reviewed for this project, settlement provisions are found in the National Payment System Act or the National Payment System Bill. Mauritius is the notable exception, as the country does not have a National Payment System Act or Bill.

Netting Arrangements: The provisions found in law should permit payment netting in clearing and settlement systems and in bilateral financial contracts (including close-out netting) and ensure that the net amounts are enforceable against unwinds, especially in insolvency situations. These laws govern netting and unwinding procedures, and define the rights and obligations of participants in the netting scheme and protect the settlement account at the Central Bank or commercial banks from stays of execution (“freezes”) upon the insolvency of a participant in a payment system. Where novation is used, laws ensuring the legal enforceability of novation (preferably through legislation) could be introduced. These provisions are more often than not found in the National Payment System Act / Payment System Management Act in each SADC country.

Official Currency: This law should establish the official currency issued or backed by the Central Bank and regulate the acceptance of currency for payment with regard to denominations relative to transaction value and eligible transactions (i.e. legal tender laws). In most SADC countries, this matter is contained in the Central Bank Law. These laws should also prohibit and penalise counterfeiting of the official currency and money laundering, and authorise monitoring and reporting of suspicious payments. These issues are generally covered in the Central Bank Act and the Anti-Money Laundering or Financial Intelligence Centre Act in all fourteen SADC jurisdictions.

Cheque or negotiable instrument: Laws and regulations should contain provisions governing the issuance, acceptance and negotiation of cheques. This may initially be governed by common law or contract but should eventually be governed by legislation. These laws should also determine the rights and obligations of payers and payees in situations of fraud as part of the criminal code or the cheque law; and enable electronic cheque presentment, truncation and imaging.

Credit transfers: Laws and regulations should authorise paper-based credit transfers and electronic wire transfers and should govern aspects such as finality of payment, misdirected payments, payment fraud and availability of funds to the customer. Several of these issues may be governed by contract and common law.

Card instrument: Card laws and regulations govern the rights and obligations of the issuer, cardholder and merchant if not covered by existing contract law. This subject may be left entirely to contract and common law or subjected to legislation to govern some aspects of the relationships such as consumer protection law.

Electronic money: These laws and regulations govern the issuance and use of electronic money and ensure the legal discharge of payment obligations through settlement by electronic money if this is not covered under currency laws. The European Union has issued Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions covering this subject matter.

Payment service: Directive 2007/64/EC Payment Services in the Internal Market is known as the Payment Services Directive or PSD and is a good example of what should be included in a payment services law. The Directive covers inter alia: the authorisation of payment institutions; own funds requirements; safeguarding requirements; the use of agents, branches or entities to which activities are outsourced; transparency of conditions and information requirements for payment services (single transactions and framework contracts); and the rights and obligations in respect to the provision and use of payment services.

Securities settlement system: The legal framework for securities settlement systems requires laws and regulations that support the immobilisation, ownership, transfer and pledging of securities (or interests in securities) in book-entry form in a securities depository or other securities intermediaries. The legislation should also support the issuance, ownership and transfer of “dematerialised” or “non-certificated” securities embodied in electronic media rather than paper. The law should mandate arrangements for Delivery versus Payment (DvP), Payment versus Payment (PvP), or Delivery versus Delivery (DvD). Legislation or contracts that validate the underlying transactions in securities, such as financial derivatives, repurchase agreements, securities loans and other transactions with regard to custody transfer and pledge of the underlying securities are preferable.

Evidence or electronic communications and transactions: These laws and regulations provide evidentiary proof of authentication of electronic payments using digital signatures or other instruments for electronic payment authorisation. The law should also provide for the establishment and maintenance of a register of cryptography providers and the accreditation of authentication products and services in support of advanced electronic signatures by a recognised Accreditation Authority.

Anti-Money Laundering and Counter Terror Financing (AML/CFT): AML/CFT laws and regulations are a vital component of the legal and regulatory framework for payments. The 2012 Financial Action Task Force (FATF) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations contain several recommendations that have direct applicability to payment systems. These include: Recommendation 10, Customer Due Diligence; Recommendation 11, Record Keeping; Recommendation 12, Politically Exposed Persons; Recommendation 13, Correspondent Banking; Recommendation 14, Money or Value Transfer Services; Recommendation 15, New Technologies; Recommendation 16, Wire Transfers; Recommendation 17, Reliance on Third Parties; Recommendation 18, Internal Controls and Foreign Branches and Subsidiaries; Recommendation 19, Higher-risk Countries; Recommendation 20, Reporting of Suspicious Transactions; Recommendation 21, Tipping-off and Confidentiality and Regulation 26, Regulation and Supervision of Financial Institutions. Countries should ensure that the legal framework, in particular the Anti-Money Laundering and Counter Terrorist Financing Law and the Financial Intelligence Centre Law (should such be in place) are compliant with the FATF Recommendations. AML provisions should, where applicable also be included in other legislation and regulation such as any instruments covering correspondent banking, the use of agents, wire transfers and remittance services.

Competition: Competition law and regulation should contain provisions establishing current jurisdiction of the Competition Authority with other regulatory authorities such as the Central Bank, mandate the competition Authority to enter into MOU's with sector specific regulators, thereby ensuring coordination and harmonisation of matters relating to competition by all regulators. Provisions on restrictive horizontal practices, restrictive vertical practices, abuse of dominance and exemptions should also be contained in the law. Competition laws have particular relevance to practices within the retail payments industry and may have a direct bearing on the regulatory approach to interchange, the existence of the so called no surcharge rule, concerted practices such as price fixing, exclusionary practices such as tying and access matters such as interoperability and membership rules.

Consumer Protection: Consumer protection is increasingly recognised as a fundamentally important issue in the ambit of the provision of payment services and the issuing of payment instruments to the public. Title III, Title IV of Directive 2007/64/EC Payment Services in the Internal Market (PSD) provide a good example of consumer protection the provisions that should be included in retail payment related laws and regulations.

4.2 Legislation and Regulation (Overarching Gap Analysis)

This section of the report provides a high-level gap analysis highlighting legislation (Acts) and regulations that are legally enforceable in each SADC Member State, draft bills and bills that have been drafted but are not legally enforceable, as they have not been tabled in Parliament or assented to and signed.³²⁰ Where no legally enforceable law or regulation is in place, this gap is highlighted. For the purposes of this study, laws and regulations are divided into “core” and “general application” laws and regulations. Core laws and regulations refer to those instruments that have a direct bearing upon the activities of FMI’s. This group of core laws and regulations consists of:

- 1) the Central Bank Act,
- 2) the Bank Act,
- 3) the Financial Institutions Act,
- 4) the National Payment System Act,
- 5) Bills of Exchange Act,
- 6) Electronic Money Act,
- 7) Payment Services Act,
- 8) Securities Act,
- 9) Stock Exchange Act,
- 10) CSD Act,
- 11) Exchange Control Act,
- 12) Electronic Communications and Transmissions Act,
- 13) Anti-Money Laundering (AML) Act,
- 14) Countering the Financing of Terrorism (CFT) Act and
- 15) the Financial Intelligence Centre (FIC) Act.

In several countries, the AML, CFT and FIC Acts are amalgamated into one general AML Act or FIC Act.






³²⁰ See Parliamentary Counsel’s Office 2011 *How to Read Legislation, A Beginner’s Guide 2* where the difference between Acts (primary legislation) and Regulations (Subsidiary or Subordinate Legislation) is explained as, “Acts are laws Parliament has enacted. Sometimes Acts are called ‘Acts of Parliament’. Less often Acts are called ‘primary legislation’ to distinguish them from subsidiary legislation. Usually they each have the word ‘Act’ in their title. An Act has to be read with any subsidiary legislation that has been made using powers in the Act to make subsidiary legislation. Subsidiary legislation will often fill in details not covered by the Act under which it is made. Not all Acts have or need subsidiary legislation. Subsidiary legislation is law made by people using powers that Parliament, by means of its Acts, has given them. Sometimes these laws are called delegated legislation or subordinate legislation [...] Subsidiary legislation does not have the words ‘subsidiary legislation’ in its title. Subsidiary legislation has various names, which do appear in its titles, such as regulations; local laws; by-laws; planning schemes; rules [...] Subsidiary legislation is made ‘under’ an Act because it is only an Act that can give a person power to make subsidiary legislation. Acts that say someone can make subsidiary legislation say who can make it and say what things the subsidiary legislation can deal with. A person making subsidiary legislation must not exceed the powers they have to make it. If they do, the subsidiary legislation will not be valid.”

The laws of general applicability relevant to the analysis in the report are:

- 1) the Company Act,
- 2) Competition Act,
- 3) Insolvency Act,
- 4) Access to Information Act, and
- 5) the Consumer Protection Act.

Table 21 below presents the symbols used in the tables throughout this report and 14 Country Annexures.

Table 21: Key

Tables (Symbols)		Diagrams (Shading)	
✓	Enforceable Act / Provision		Enforceable Act / Provision
✓	Enforceable Regulation / Determination / Directive		Enforceable Regulation / Determination / Directive Enforceable Regulation
*	Provisions Incorporated into Another Act (No Stand Alone Act)		Provisions Incorporated into Another Act (No Stand Alone Act)
●	Bill or Provisions found in a Bill of Draft Bill (Not Enforceable)		Bill or Provisions found in a Bill of Draft Bill (Not Enforceable)
✗	Nothing in Place (Gap)		Nothing in Place (Gap)
P(A)	Unknown		

As depicted in Table 22 below, SADC Member States are at different stages of development of their legal and regulatory frameworks for payments. For the purposes of this project, the primary gap highlighted is that the DRC, Lesotho, Malawi and Tanzania do not have a legally enforceable National Payment System Act in place. All four of these countries are at varying stages of the legislative process with respect to having their Bills tabled and promulgated. Mauritius is the only country that has not drafted a National Payment System Bill. All five of these countries are therefore exposed in terms of there being no legally enforceable law in place governing vital issues such as insulation of collateral security from the effects of insolvency, settlement finality and irrevocability, Central Bank oversight and supervision of the National Payment System. Some of these provisions are contained in settlement system and ACH Rules, Terms and Conditions and Policies and Procedures, however, it preferable that these provisions are set down in law and not in bi-lateral agreements. In Mauritius for example, provisions on settlement finality and irrevocability and money settlements in central bank money are not included in Mauritian Law or Regulations. This is an area of great concern as the only references to finality and irrevocability are found in the Port Louis Automated Clearing House Rules and the Mauritius Automated Clearing and Settlement System Terms and Conditions. The reliance on these bi-lateral arrangements between participants' results in an ad-hoc self-regulated payments industry, a situation that should not be left unchecked by the Central Bank. As the payment systems are maturing in the DRC, Lesotho, Malawi, Tanzania and Mauritius, it is vital that the Bills that have, in some cases been outstanding for more than ten years, are passed. In the case of Mauritius, legislation in the form of a National Payment System Act should be introduced as soon as is reasonably practicable, so as to allow for more formalised regulation.³²¹

³²¹ Volker *Essential Guide to Payments: An Overview of the Services, Regulation and Inner Workings of the South African National Payment System*.

The formal regulation of electronic money (E-Money) and payment services is very poor in all 14 SADC Member States. Only two countries, the DRC and Namibia have issued a legally enforceable determination (Namibia) and directive (DRC) on the matter. Most SADC Member States do not have a well-structured legal and regulatory framework for retail payments. In all 14 SADC countries, vital issues such as card payments, agent banking, the authorisation of payment service providers, the issuance of payment instruments and the rights and obligations of PSPs and users are, in the most part, set out in guidance notes, guidelines and position papers. These by their very nature are not legally enforceable and the Central Bank as the sector regulator generally has no powers, other than moral suasion to enforce them.

In recognition of the growing importance of retail payments and the need to harmonise domestic law in this area, the European Parliament and the Council adopted Directive 2007/64/EC Payment Services in the Internal Market (PSD) otherwise known as the Payment Services Directive in November 2007. Member States had until 1 November 2009 to transpose the Directive into National Law. None of the fourteen SADC Member States have such a law in place, although some of the provisions found in the PSD have been included in the DRC's Draft Law on the Provisions Applicable to the National Payment System.³²²

Another area of concern is the fact that only four countries have promulgated a separate Electronic Communications and Transmissions Act. While some provisions on the *prima facie* nature of electronic documents have been included in the National Payment System Act in several countries³²³, vital provision on for example, evidentiary proof of authentication of electronic payments using digital signatures or other instruments for electronic payment authorisation, the establishment and maintenance of a register of cryptography providers and the accreditation of authentication products and services in support of advanced electronic signatures by a recognised Accreditation Authority are not covered by law and regulation.

Only two of the fourteen SADC Member States have a stand-alone Central Securities Depository Act. In general, the issue of the regulation of the payments leg of securities transactions is not well covered in law and regulation. Mozambique and Angola are the only two SADC Member States that include a provision on the finality and irrevocability of securities settlements in their National Payment System Acts.³²⁴

³²² The drafters of the DRC's Draft Law on Provisions Applicable to the National Payment System, 2013 appear however to have been highly selective in terms of which PSD provisions they have incorporated into their draft domestic law. Important provisions such as the definition of payment service providers, payment institutions, capital requirements, own funds, safeguarding requirements, authorisation of payment institutions, information requirements for and single payment transactions have been left out of the draft law.

³²³ The DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 for example, contains several provisions on electronic documents, transactions and signatures. Articles 62 to 66 cover 1) payment orders kept in archives in electronic format constitute proof and are legally admissible, 2) writing in electronic format is accepted as proof; 3) documents in electronic format must be kept for a period of 10 years, 4) secure electronic signature linked to an electronic certificate are accepted as and carry the evidentiary weight as handwritten signatures, 5) institutions who would like to set up or operate an electronic certification system must be approved by the Central Bank. It is however recommended that in the absence of an Electronic Transactions and Communications Act that the DRC consider revising these provisions by using the UNCITRAL Model Law on Electronic Commerce (1996) as a best practice benchmark.

³²⁴ Article 20 of the Mozambican Law 02/08 of 27 February reads, "(1) In operations involving securities, final settlement through the transfer of funds shall be effected in accordance with the provisions of Article 18 of this law. (2) Without prejudice to the regulations governing securities and other regulations issued by the securities exchange as concerns operations mentioned in the paragraph above, the settlement of funds transfer and the settlement of securities transfer shall occur simultaneously in accordance with the principle of delivery versus payment. (3) When the principle of delivery versus payment, as provided in the paragraph above, is impossible to adhere to, additional credit and liquidity risk measures shall be adopted in respect of the clearing and settlement of operations in securities markets."

All fourteen SADC Member States have comprehensive AML/CFT legal and regulatory frameworks in place. Several countries have elected to promulgate one Act that covers AML, CFT and the operations of a Financial Intelligence Centre. Others, such as Namibia and South Africa have split these matters into three different statutory instruments.³²⁵

³²⁵ Desk based research and in-country interviews with relevant stakeholders show substantial improvements having been made by all fourteen SADC member countries to their AML/CFT legal and regulatory regimes post the first round of ESAAMLG Mutual Evaluations and highlights the need for the reports to be updated making use of the revised 2012 recommendations and a standardised assessment methodology. It is also essential that the next round of evaluations produce reports that are factually correct, based upon the homogenous and accurate interpretation of the FATF Recommendations and that such assessments are objective and fair.

Table 22: Core Acts in Force in Each SADC Country

CORE ACTS	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW
Central Bank Act	✓	✓	●	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●
Banking Act	* 326	✓	●	* 327	✓	✓	* 328	✓	* 329	●	* 330	✓	✓	✓
Financial Institutions Act	✓	✓	✗	✓	✓	✓	✓	●	✓	✓	✓	* 331	* 332	✗
National Payment System Act	✓	✓	●	●	●	✗	✓	✓	✓	✓	✓	●	✓	✓
Bills of Exchange Act	✗	✓	✓	✗	✓	✓	* 333	✓	✓	✓	✗	✓	✓	✓
Electronic Money Act	✗	✗	* 334	✗	✗	✗	* 335	* 336	✗	✗	✗	✗	✗	✗
Payment Services Act	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Securities Act	✓	●	✓	✗	✓	✓	✓	●	✓	✓	✓	✓	✓	●
Stock Exchange Act	✗	✓	✗	✗	* 337	* 338	✓	✓	* 339	* 340	* 341	* 342	* 343	* 344
CSD Act	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	●	✗	✗
Exchange Control Act	✓	NA	✓	✓	✓	NA	✓	✓	✓	✓	✓	✓	✓	✓

³²⁶ Law n° 13/05.

³²⁷ Financial Institutions Act 3 of 2012.

³²⁸ Law n° 15/99 of 1 November Law on Credit Institutions and Finance Companies As amended by Law 9/2004 of 21 July

³²⁹ Financial Institutions Act, 2004 (As Amended).

³³⁰ Financial Institutions Act 6 of 2005.

³³¹ Banking and Financial Institutions Act 5 of 2006.

³³² Banking and Financial Services Act (Vol 21 ch 387).

³³³ Decree Law n° 2/2005 of December 27 (Commercial Code of Mozambique).

³³⁴ Directive 24 on Electronic Money.

³³⁵ Law n° 15/99 of 1 November Law on Credit Institutions and Finance Companies As amended by Law 9/2004 of 21 July.

³³⁶ Payment System Determination on Issuing of Electronic Money in Namibia (PSD-3), 2012.

³³⁷ Securities Act 20 of 2010.

³³⁸ Securities Act 22 of 2005.

³³⁹ Securities Act 8 of 2007.

³⁴⁰ Financial Markets Act 19 of 2012.

³⁴¹ See Securities Act 9 of 2010.

³⁴² Capital Markets And Securities Act 5 of 2004.

³⁴³ The Securities Act [Chapter 354].

³⁴⁴ Securities Act, 2004.

Electronic Communications & Transmissions Act	* 345	●	✘	✘	●	✓	* 346	●	✓	✓	✘	● *	✓	* 347
AML Act	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CFT Act	✓	●	* 348	* 349	* 350	✓	* 351	✓	✓	✓	✓	✓	✓	✓
FIU Act	* 352	✓	* 353	* 354	* 355	* 356	✓	✓	* 357	✓	* 358	* 359	✓	* 360

Table 23 below shows that all fourteen SADC Member States have a Companies Act in place, only three (Angola, the DRC and Lesotho) have not promulgated a Competition Act and several do not have an Access to Information Act in place. For the purposes of this study, the fact that several SADC Member States do not have a legally enforceable Consumer Protection Act in place is highlighted as a major gap. It is also important to note that none of the countries that do have a Consumer Protection Act in place include payment specific provisions on framework contracts and once off transactions in their Acts. It is recommended that this gap be rectified through the development of a Model Law on Payment Services that could then be transposed into domestic law in each SADC country.

In the absence of provisions covering international arbitration in the National Payment System Act of each SADC Member State, the provisions found in an International Arbitration Act and an Implementing Act of the Convention on the Enforcement of Foreign Arbitral Awards becomes essential. As indicated in Table 19 below, the legal and regulatory framework in several SADC Member States is deficient in this regard.

Table 23: Acts of General Application in Force in Each SADC Country

GENERAL APPLICATION	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW
Company Act	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Competition Act	●	✓	✘	✘	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

³⁴⁵ Related Act, Basic Telecommunication Law, 2001.

³⁴⁶ Law n° 22/92 Telecommunications Act (Related Act).

³⁴⁷ Related Laws: The Postal and Telecommunications Act 4 of 2000; Interceptions of Communications Act, 2008; Access to Information and Protection of Privacy Act, 2004.

³⁴⁸ Loi No. 04/016 du 19 Juillet Portant Lutte Contre le Blanchiment Des Capitaux et le Financemet du Terrorisme.

³⁴⁹ Money Laundering and Proceeds of Crime Act 4 of 2008.

³⁵⁰ Money Laundering Proceeds of Serious Crime and Terrorist Financing Act 1 of 2006.

³⁵¹ Law n° 14/2013 of 12 August Anti-Money Laundering and Combatting of Terrorist Activities.

³⁵² Law n° 34/11.

³⁵³ Loi N° 04/016 du 19 Juillet Portant Lutte Contre le Blanchiment Des Capitaux et le Financemet du Terrorisme.

³⁵⁴ Money Laundering and Proceeds of Crime Act 4 of 2008.

³⁵⁵ Money Laundering Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006.

³⁵⁶ Financial Intelligence and Anti-Money Laundering Act 6 of 2002.

³⁵⁷ Anti-Money Laundering Amendment Act 18 of 2008 and Anti-Money Laundering (Amendment) Act 24 of 2011.

³⁵⁸ Money Laundering and Financing of Terrorism (Prevention) Act, 2011.

³⁵⁹ Mainland Tanzania: Anti-Money Laundering Act, 2006 (As Amended); Tanzania Zanzibar: Anti Money Laundering and Proceeds of Crime Act, 2009 for Tanzania Zanzibar (As Amended).

³⁶⁰ Money Laundering and Proceeds of Crime Act 4 of 2013.

Insolvency Act	✓	✓	✓	✓	●	✓	✓	✓	✓	✓	✓	* 361	✓	✓
Access to Information Act	✓	●	✗	●	●	✗	●	✗	✗	✓	✗	●	●	✓
Consumer Protection Act	✓	✓	✗	● 362	✓	✓	✓	✗	✓	✓	●	✗ 363	✓	✓
Arbitration Act (Domestic)	✓	✓	✓	✓	✓	* 364	✓	✓	* 365	✓	✓	✓	✓	✓
Implementing Act of the Convention on the Enforcement of Foreign Arbitral Awards	✗	✓	?	✓	✗	✓	✓	✗	✗	✓	✗	✗	✓	✗

4.3 Strong Legal Influence (National Payment System Acts)

As shown in Diagram 9 below, the review of the National Payment System Act / Payment System Management Act or Bill in each SADC country has shown a certain level of harmonisation in specific groupings of countries. Mauritius, being the only country in the SADC that has elected not to enact a National Payment System / Payment System Management Act is not included in this Diagram. Tanzania is also not included as although Tanzania has embarked upon the process of drafting a National Payment System Bill, at the time of publication of this report, the draft Bill was not at the stage where it could be shared with stakeholders and the general public for comment. The Bank of Tanzania has advised that the Bill is currently with the Acting Minister (Minister of Finance) and will soon be tabled. It is important to note, as stated by the Bank of Tanzania that the “basis of the proposed Act has the same spirit enshrined in the powers and functions of Bank of Tanzania under Section 6 of the Bank of Tanzania Act. The proposed National Payment System Act will consider the same issues considered by other jurisdictions while enacting their National Payment System laws. Wider consultation was done and experience from other jurisdictions also considered.”³⁶⁶

³⁶¹ Companies Act, 2002.

³⁶² Require clarification on whether this has been enacted.

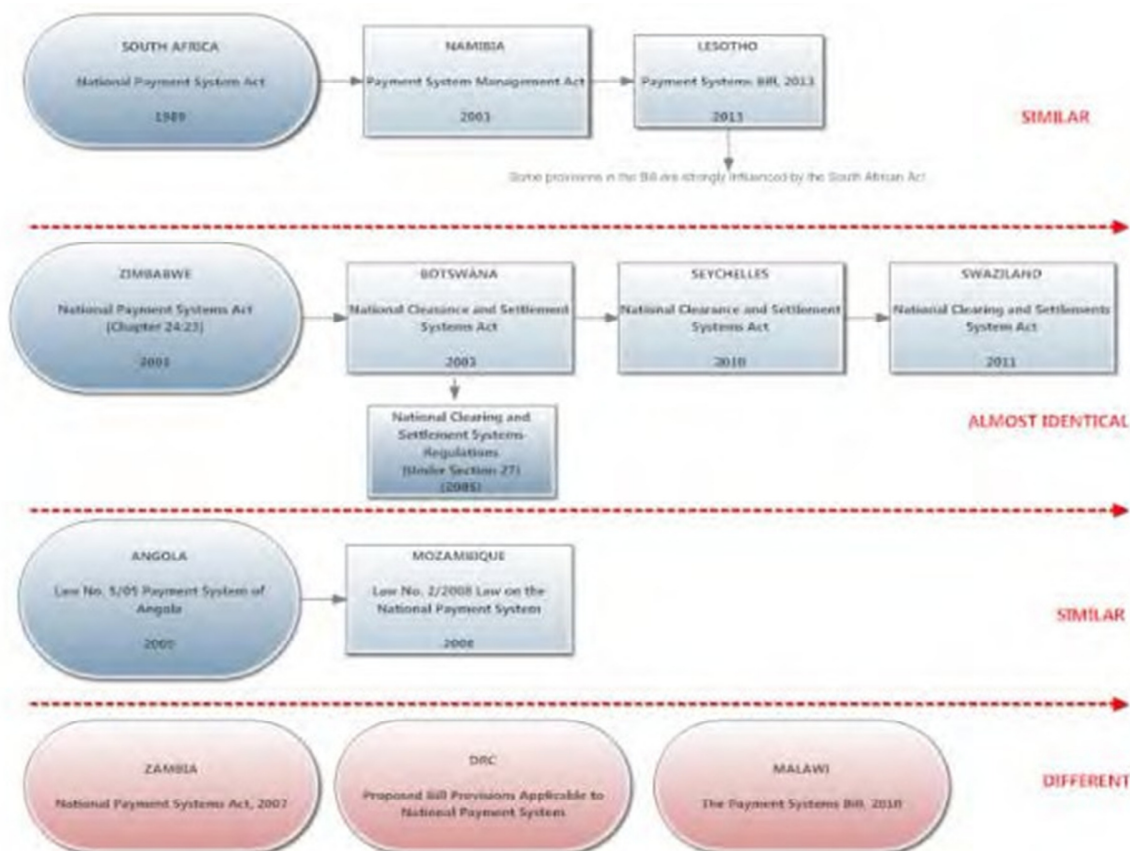
³⁶³ Tanzania to please confirm whether there is a Consumer Protection Bill or Act.

³⁶⁴ *Code de Procédure Civile*.

³⁶⁵ Provisions found in the Commercial Code Act.

³⁶⁶ Statement made on behalf of the Bank of Tanzania (01/04/2014).

Diagram 9: Strong Legal Influence (Similar Acts)



Source: Authors own representation

Although legislation sets out laws, not all of the words in legislation are part of the law. Headings to sections such as “Powers of the Central Bank” are not part of the law and it is usually unwise to rely on a section’s heading to interpret what is in the section. A heading is however meant to be a short pointer to the subject matter of the section.³⁶⁷ While a section’s heading almost never conveys accurately or fully what is in the section, in the analysis that follows in this section of the report, the headings of sections found in the National Payment System Act in each SADC country have been used for the purpose of comparing the manner in which each Act is structured and drafted.

4.3.1 Similar Acts: South Africa, Namibia and Lesotho

As represented in Table 24 below, the structure of the National Payment System Act in South Africa, Namibia and Lesotho is similar. The Namibia Payment System Management, 2003 (As Amended)³⁶⁸ however contains two provisions that are not found in the South African National Payments System Act, 1998 (As Amended)³⁶⁹ namely, indemnity (Section 12) and the power of the Bank to, by notice in the Gazette, make determinations not inconsistent with this Act (Section 14). Determinations are not defined in the Namibian Act, but have the

³⁶⁷ See Parliamentary Counsel’s Office *How to Read Legislation, A Beginner’s Guide*.

³⁶⁸ Act 18 of 2003 (As Amended).

³⁶⁹ Act 78 of 1998 (As Amended).

same force of law as Regulations.³⁷⁰ Several provisions in Lesotho’s Payment Systems Bill, 2013 have been influenced by the South African National Payments System Act, 1998³⁷¹, particularly the provisions relating to the Payment System Management Body. However, this Bill appears to also contain provisions found in other Act in force in the Region. An example of this are Section 26 on the admissibility of electronic and optical evidence, a provision not found in South Africa or Namibia’s Payment System Act. Lesotho is also the only country in the SADC Region that has elected to make use of a licensing regime instead of the typical designation or recognition approach.³⁷² The Bill does not refer to “designation” or recognition of systems. Instead, Section 9 reads, “a person shall not operate a system in Lesotho, unless the person is in the possession of a licence for this purpose, obtained from the Central Bank.” Lesotho’s Bill contains dedicated Parts on insolvency (Part V) and collateral arrangements (Part VI), but does not, unlike the South African and Namibian Acts respectively; contain provisions on confidentiality, indemnity, the settlement of disputes, and the retention of records or application for a court order.

Table 24: Comparing the Structure and Content of the National Payment System Act in South Africa, Namibia and Lesotho

Section	South Africa		Namibia		Lesotho	
	Ref		Ref		Ref	
Definitions	S1	✓	S1	✓	S2	●
Object of the Act					S3	●
Oversight	-	✗	-	✗	S1, 373	●
Powers and duties of Reserve Bank regarding payment system	S2	✓	S2	✓	S4 ³⁷⁴	●
Payment system management body	S3	✓	S3	✓	S5	●
<i>Recognition and membership of the Body</i>	S3	✓	S3	✓	S6	●
<i>Withdrawal of recognition</i>	S3	✓	S3	✓	S7	●
Objects and rules of payment system management body	S4	✓	S3	✓	S8 ³⁷⁵	●

³⁷⁰ In Namibia, Determinations are gazetted and whereas Directives are not. The process for issuing these two types of instruments is different. Both Directives and Determinations are drafted by the Bank of Namibia, are then subject to an internal review process and submitted to the Governor’s Office for approval. At this point, the Bank may issue the Directive directly. Determinations must however be sent to the Minister of Justice for review and are then gazetted.

³⁷¹ Act 78 of 1998 (As Amended).

³⁷² See Le Sar B and Porteous D 2012 *Introduction to the National Payments System* 32 where the authors note that, “a payments system usually became subject to regulation as a result of the regulator designating it. The effect of designation was to bring the system under a set of regulations that gave regulators the power: to vet the payments system’s rules and procedures to ensure they were adequate, and to review any changes in advance; to require that governance structures, including the identity of owners or individuals on the board or governing committees of payments systems, met appropriate standards; to review risk procedures, including disaster recovery, and to require changes if necessary; and to require that regular reports be submitted. The designation approach was based on an understanding that the key function of regulation was to manage systemic risk; and that excess regulation of lower risk systems would hamper the ability of payments systems to innovate. The concept of designation remains important, giving payment regulators the power to subject a designated system to additional scrutiny and control. All SIPSs are subject to this heightened level of regulation.”

³⁷³ Lesotho’s National Payment System Bill, 2013 differs from the South African and Namibian Acts in that it contains a specific section on oversight.

³⁷⁴ Section 4 of Lesotho’s National Payment System Bill, 2013 refers to the “functions of the Governor of the Central Bank” and not the powers, duties and functions of the Bank with respect to the National Payment System as is the case with the Namibian and South African Acts.

³⁷⁵ Section 8 of Lesotho’s National Payment System Bill, 2013 refers is titled “functions of the body”.

Designated settlement systems	S4A	✓	S4	✓	-	✗
Licensing ³⁷⁶	-	✗	-	✗	S ₀ ³⁷⁷	●
Settlement provision	S5	✓	S4	✓	S30	●
Clearing provisions and designated clearing system participants	S6	✓	S6	✓	S31	●
Effectiveness and efficiency of the National Payment System	S6A	✓	-	✓ ³⁷⁸	-	✗
Payments to third persons	S7	✓	S ₇ ³⁷⁹	✓	S29	●
Curatorship, judicial management or liquidation	S8	✓	S8 ³⁸⁰	✓	S17 & 18	●
Utilisation of assets provided as security	S9	✓	S9	✓	S20 - 25	●
Information	S10	✓	S10	✓	S ₁₄ ³⁸¹	●
Confidentiality	S10	✓	S11	✓	-	✗
Indemnity	-	✗	S12	✓	-	✗
Settlement of disputes	S11	✓	S15	✓	-	✗
Directives by Reserve Bank	S12	✓	S13	✓	S15	●
Determinations / Regulations	-	✗	S14	✓	S33	●
Retention of records	S13	✓	S16	✓	-	✗
Application for court order	S13A	✓			-	✗
Evidence	-	✗	-	✗	S26 & S27	●
Penalties	S14	✓	S17	✓	S ₁₆ ³⁸²	●
Review of Act	S15	✓				●
Short title	S16	✓	S18	✓	S1	●

³⁷⁶ See Le Sar and Porteous *Introduction to the National Payments System* 32 where the authors note that, “as the reach of payments systems has extended to touch more people, a recent trend has been to cast the net of regulation more broadly over payments systems, whether systemically important or not. In general, two approaches are increasingly common: All payments systems must be licensed and therefore subject to oversight (Rwanda and India’s Acts, passed in 2007 and 2010 respectively, require this); or all payments systems must be registered, but only designated systems are subject to direct oversight. Note that licensing per se does not subject a system to high intensity oversight, as designation does, but it does at least mean that the regulator will oversee the system.”

³⁷⁷ Lesotho is the only country in SADC that has elected to make use of a licensing regime. The Bill does not refer to “designation” or recognition of systems. Instead, Section 9 reads, “a person shall not operate a system in Lesotho, unless the person is in the possession of a licence for this purpose, obtained from the Central Bank.”

³⁷⁸ This is specifically addressed in PSD-7. Additionally, the Payment System Management Amendment Act, 2010, defines and deals with “cost-effectiveness” while Section 13 of the Payment System Management Act, 2003, also allows for the issuing of Directives in the interest of effectiveness.

³⁷⁹ Section 7 of the Namibian Payment System Management Act 18 of 2003 (As Amended) is entitled “payment intermediation” and not “payment to third persons” as is the case in the South African Act.

³⁸⁰ Section 8 of the Namibian Act is entitled “netting agreements and netting rules” and not “curatorship, judicial management or liquidation” as is the case in the South African Act.

³⁸¹ Section 14 of Lesotho’s Payment Systems Bill, 2013 covers the investigative powers of the Governor and covers access to information, on-site inspections and the seizure or taking of copies of relevant documentation.

³⁸² Section 16 of Lesotho’s Payment Systems Bill, 2013 is a comprehensive provision on sanctions.

4.3.2 Almost Identical Acts: Botswana, Seychelles and Swaziland

The influence of Zimbabwe’s National Payment Systems Act [Chapter 24:23] is clearly evident in Botswana’s National Clearance and Settlement Systems Act, 2003,³⁸³ the Seychelles National Clearance and Settlement Systems Act, 2010³⁸⁴ and Swaziland’s National Clearing and Settlement Systems Act, 2011.³⁸⁵ It is clear, as represented by Table 25 below that structure and substantive content of Zimbabwe’s Act was used by Botswana, Seychelles and Swaziland as the template for their domestic law as the provisions are almost identical. Botswana, Seychelles and Swaziland have however improved on the original content of Zimbabwe’s National Payment Systems Act [Chapter 24:23] and added additional sections and incorporated several domestic nuances. Botswana for example, included specific provisions not found in the Zimbabwean Act on: unpaid items due to insufficient funds (Section 23), computer entries (Section 24), imaging (Section 25) and the Ministers power to make regulations providing for the better carrying out of the provisions of the Act (Section 27) in their National Clearance and Settlement Systems Act, 2003.³⁸⁶ The Seychelles National Clearance and Settlement Systems Act, 2010³⁸⁷ contains a provision of record keeping not found in the Zimbabwean, Botswana or Swaziland Acts. Seychelles has also derogated from the Zimbabwe and Botswana Acts through the insertion of sections 11(1) and 11(2) into the National Clearance and Settlement Systems Act, 2010.

Swaziland also appears to have drawn heavily upon the Botswana Act as a template as the Swaziland Act more closely resembles that Botswana Act than the Zimbabwean Act. Seychelles appears to have used the Botswana National Clearance and Settlement Systems, 2003³⁸⁸ as the template for their National Clearance and Settlement Systems Act, 2010³⁸⁹ as the structure and content of the Seychelles National Clearance and Settlement Systems Act, 2010 more closely resembles the Botswana Act than the Zimbabwe Act.

The Bank of Botswana, realising that the National Clearance and Settlement Systems Act, 2003³⁹⁰ did not cover several important provisions, issued the National Clearance and Settlement Systems Regulations, 2005, to rectify some of these gaps. Botswana’s Regulations cover *inter alia*: application for a certificate of recognition (Regulation 3), conditions for recognition (Regulation 4), investigation of unrecognised systems (Regulation 7), rules and procedures of management bodies (Regulation 14), and offences and penalties (Regulation 18).

Table 25: Comparing the Structure of the National Payment System Act and Regulations in Zimbabwe, Botswana, Seychelles and Swaziland

	Zimbabwe		Botswana		Seychelles		Swaziland	
	Ref		Ref		Ref		Ref	
PART I PRELIMINARY								
Short title	S1	✓	S1	✓	S1	✓	S1	✓
Interpretation	S2	✓	S2	✓	S2	✓	S2	✓
PART II PAYMENT AND SETTLEMENT SYSTEMS								

³⁸³ Act 5 of 2003.

³⁸⁴ Act 12 of 2010.

³⁸⁵ Act 17 of 2011.

³⁸⁶ Act 5 of 2003.

³⁸⁷ Act 12 of 2010.

³⁸⁸ Act 5 of 2003.

³⁸⁹ Act 12 of 2010

³⁹⁰ Act 5 of 2003.

Application for recognition of a clearance and settlement system	-	×	Regs.	*	S ₃ ³⁹¹	✓	-	×
Recognition of payment systems	S ₃	✓	S ₃ ³⁹²	✓	S ₄ ³⁹³	✓	S ₃ ³⁹⁴	✓
Approval of amendments to constitution and rules of recognised payment system	S ₄	✓	S ₄	✓	S ₅	✓	S ₅	✓
Constitution and rules of recognised payment system to be open to inspection	S ₅	✓	S ₅	✓	S ₆	✓	S ₄	✓
Withdrawal of recognition from payment system	S ₆	✓	S ₆ ³⁹⁵	✓	S ₇	✓	S ₆	✓
Establishment and operation of settlement system	S ₇	✓	S ₇	✓	S ₈	✓	S ₇	✓
Discharge of settlement obligations within settlement system	S ₈	✓	-	×	-	×	-	×
Provision of information to Reserve Bank	S ₉	✓	S ₈	✓	S ₉	✓	S ₈	✓
Control of undesirable conduct in regard to recognised payment system ³⁹⁶	S ₁₀	✓	S ₉	✓	S ₁₀	✓	S ₉	✓
PART III FINALITY OF SETTLEMENTS WITHIN RECOGNISED PAYMENT SYSTEM OR SETTLEMENT SYSTEM								
Finality of payments and transfers made within settlement system	S ₁₁	✓	S ₁₀	✓	S ₁₁	✓	S ₁₀	✓
Payments and transfers within settlement system not subject to interdict or stay	S ₁₂	✓	S ₁₁	✓	-	×	S ₁₁	✓
PART IV WINDING UP, JUDICIAL MANAGEMENT OR CURATORSHIP OF PARTICIPANTS IN RECOGNISED PAYMENT SYSTEM								
Reserve Bank to be notified of winding up or judicial management of participant in recognised payment system	S ₁₃	✓	S ₁₂	✓	S ₁₃	✓	S ₁₂	✓
Winding up or judicial management of participant in recognised payment system not to affect finality of prior settlements	S ₁₄	✓	S ₁₃	✓	S ₁₂	✓	S ₁₃	✓
Rules, etc., of recognised payment system binding on liquidator, judicial manager or curator	S ₁₅	✓	S ₁₄	✓	S ₁₄	✓	S ₁₄	✓
Priority of certain instruments on winding up of participant in recognised payment system.	S ₁₆	✓	S ₁₅	✓	S ₁₅	✓	S ₁₅	✓
PART V GENERAL								
Prohibition against unrecognised payment systems	S ₁₇	✓	S ₁₆	✓	S ₁₆	✓	S ₁₆	✓
Prohibition against payment intermediation	S ₁₈	✓	S ₁₇	✓	S ₁₇	✓	S ₁₇	✓

³⁹¹ Regulations found in the Botswana National Clearance and Settlement Systems Regulations, 2005 are incorporated into the legal text of the Seychelles National Clearance and Settlement Systems Act 12 of 2010.

³⁹² Botswana's National Clearance and Settlement Systems Act, 2003 refers to the recognition of clearance and settlement systems not "payment systems" as the Zimbabwean Act does. The wording used in Section 3 of both Acts is however almost identical and refers to clearing and settlement systems.

³⁹³ The Seychelles National Clearance and Settlement Systems Act, 2010 also refers to the recognition of clearance and settlement systems and not "payment systems" as the Zimbabwean Act does, showing the likelihood that the Botswana Act was used as the template by Seychelles.

³⁹⁴ The Swaziland National Clearing and Settlements System Act, 2011 also refers to the recognition of "clearing and settlement systems" and not "payment systems" as the Zimbabwean Act does.

³⁹⁵ Botswana refers to the "withdrawal of recognition from clearance and settlement systems" whereas the Zimbabwean Act refers to "payment systems".

³⁹⁶ This provision refers to the power of the Central Bank to issue Directives.

Settlement of disputes arising out of recognised payment system or settlement system	S19	✓	S18	✓	S18	✓	S18	✓
Exercise of functions by Reserve Bank	S20	✓	S19	✓	-	✗	S19	✓
Preservation of secrecy	S21	✓	S20	✓	S19	✓	S20	✓
Use of confidential information for personal gain	S22	✓	S21	✓	S20	✓	S21	✓
Evidence	S23	✓	S22	✓	S21	✓	S22	✓
Review of Act	S24	✓	S26	✓	-	✗	S26	✓
Unpaid items due to insufficient funds	-	✗	S23	✓	-	✗	S23	✓
Computer entries	-	✗	S24	✓	S22	✓	S24	✓
Imaging	-	✗	S25	✓	S23	✓	S25	✓
Reserve Bank to report on recognised payment systems to Minister	S25	✓	-	✗	-	✗	-	✗
Transitional provision: existing payment systems	S26	✓	-	✗	-	✗	-	✗
Records	-	✗	-	✗	S24	✓	-	✗
Regulations	-	✗	S27	✓	S25	✓	S26	✓
Botswana National Clearance and Settlement Systems Regulations, 2005								
Application for a certificate of recognition	-	✗	R3	✓	S3	✓	-	✗
Conditions of recognition	-	✗	R4	✓	-	✗	-	✗
Applicant to be incorporated in Botswana	-	✗	R5	✓	-	✗	-	✗
Certificate of recognition	-	✗	R6	✓	-	✗	-	✗
Investigation of unrecognised system, etc.	-	✗	R7	✓	-	✗	-	✗
Renewal of certificate	-	✗	R8	✓	-	✗	-	✗
Transfer of certificate	-	✗	R9	✓	-	✗	-	✗
Surrender of certificate	-	✗	R10	✓	-	✗	-	✗
Display of certificate	-	✗	R11	✓	-	✗	-	✗
Duties of the management body	-	✗	R12	✓	-	✗	-	✗
Constitution of management body	-	✗	R13	✓	-	✗	-	✗
Rules and procedure of management body	-	✗	R14	✓	-	✗	-	✗
Service level agreement of management body	-	✗	R15	✓	-	✗	-	✗
Instructions by Central Bank	-	✗	R16	✓	-	✗	-	✗
Settlement services	-	✗	R17	✓	-	✗	-	✗
Offence and penalty	-	✗	R18	✓	-	✗	-	✗

4.3.3 Similar Acts: Mozambique and Angola

The Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems and the Mozambican Law nº 2/2008 of 27 February are similar in both structure and content. This is not surprising given the similar legal systems in both countries and the use of the Portuguese language. Both the Angolan and Mozambican Acts contain a specific Article on public interest objectives. While the “public interest” is mentioned in several other National Payment System Acts in the SADC region, the Angolan and Mozambican Acts are the only two Acts that specifically list security, reliability, transparency and efficiency as public interest objectives. The Mozambican Act also contains several unique provisions not found in the Angolan Act. Article 10 of the Mozambican Law nº 2/2008 for example, establishes the National Payment System Coordinating Committee (CCSNP). This Committee is chaired by the *Banco de Moçambique* and includes representatives from: the *Banco de Moçambique*; Ministry of Finance; National Communications Institute; Mozambican Securities Exchange;

Mozambican Bankers’ Association; Commercial banks and Companies providing payment services. The powers and functions of the CCSNP is set out in Article 11.³⁹⁷ Article 17 on Payment Instruments, Transactions and Electronic Archives that is included in the Mozambican Law is not included in the Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems.³⁹⁸ In Angola, although not covered in Law nº 5/05, Joint Order nº 70/00, de 14 de Abril creates the Technical Council of the Payment Systems of Angola. This Technical Council is headed by the Angolan National Bank and is tasked with: preparing reports and making proposals related with the National Payment System, meeting the requests of the Angolan National Bank or the own initiatives of the entities represented on the Council; creating working groups for the preparation of specific projects related to the National Payment System and regularly reporting on issues analysed by the Council to the *Banco Nacional de Angola* represented entities.

Article 24 of the Mozambican Law nº 2/2008 of 27 February covers Settlement of Operations with Truncation and Article 24(1) states that “Truncation of cheques and other instruments is permitted, up to the value and under the conditions defined by the *Banco de Moçambique* upon the recommendation of the National Payment System Coordinating Committee.” The Mozambican and Angolan Acts also includes a provision on Delivery Versus Payment (DVP), a provision not found in other National Payment System Acts in the SADC Region.³⁹⁹

Table 26: Structure and Content of the Angolan and Mozambican National Payment System Acts

Section	Angola		Mozambique	
	Article		Article	
CHAPTER I: GENERAL PROVISIONS				
Purpose / Object	Article 1	✓	Article 1	✓
Definitions	Article 2	✓	Article 2	✓
Composition	-	✗	Article 3	✓
Public Interest Objectives	Article 3	✓	Article 4	✓
Fulfilment of Public Interest Objectives	Article 4	✓	Article 4	✓
CHAPTER II: ROLE PLAYERS IN THE NPS				
<i>Section I About the Role Players</i>				
Role players in the payment system	Article 5	✓	Article 5	✓
<i>Section II About the Central Bank</i>				
Central Bank Competencies /Powers and Functions	Article 6	✓	Article 6	✓
Duties of the Central Bank	Article 7	✓	Article 6	✓

³⁹⁷ Article 11 of Mozambican Law nº No 2/2008 of 27 February reads, “the CCSNP shall: a) on its own initiative or when requested of it, comment on issues related to the improvement and upgrading of the National Payment System; b) submit to the *Banco de Moçambique*, studies, suggestions or recommendations for the continuous development of the National Payment System; c) create technical sub-committees to assist with the preparation of studies and examination of specific issues concerning the National Payment System; d) fulfil other tasks as may be entrusted to it.”

³⁹⁸ Article 17 reads, “the operations provided for in this Law and regulations approved for its implementation may take on the form of electronic transactions. Electronic transactions effected in terms of this Law and all respective supporting documents and electronic archives shall have full probative force. Copies of electronic documents in an identical or different format shall be valid and have the probative force attributed to photocopies under Civil and Civil Procedure Law. The *Banco de Moçambique* shall issue specific norms on payment instruments, transactions and electronic archives used in connection with the National Payment System.”

³⁹⁹ Article 20(2) of Law nº No 2/2008 of 27 February reads, “without prejudice to the regulations governing securities and other regulations issued by the securities exchange as concerns the operations mentioned in the paragraph above, the settlement of the funds transfer and the settlement of the securities transfer shall occur simultaneously in accordance with the principle of delivery versus payment.”

Exercising Oversight	Article 8	✓	Articles 6 & 7	✓
Confidentiality of Information	Article 9	✓	Article 8	✓
Duty of Disclosure	Article 10	✓	Article 9	✓
Establishment of the National Payment System Coordinating Committee (CCSNP)	-	✗	Article 10	✓
Powers and functions of the CCSNP	-	✗	Article 11	✓
CHAPTER III SETTLEMENT OPERATIONS				
<i>Section I Final Settlement of Transfer of Funds</i>				
Finality of Settlements (Procedure)	Article 11	✓	Article 12	✓
Settlement Features (Settlement Account)	Article 12	✓	Article 18	✓
Settlement Intermediaries	Article 13	✓	Article 19	✓
<i>Section II Settlement of Operations with Securities</i>				
Principle of Delivery versus Payment	Articles 11 and 15	✓	Article 20	✓
Definition	Article 14	✓	-	✗
Procedure	Article 15	✓	-	✗
Counterparty in financial transactions	Article 16	✓	Article 21	✓
<i>Section III Security of Final Settlement</i>				
Conditions	Article 17	✓		
<i>Section IV Multilateral Netting</i>				
Definition	Article 18	✓	Article 22	✓
Mechanism for the settlement of multilateral netting / clearing	Article 19	✓	Article 23	✓
<i>Section V Participants under Special Legal Regimes</i>				
Bankruptcy or exceptional operating regimes	Article 20	✓	Article 16	✓
Performance of Guarantees	Article 21	✓	Article 14 & 15	✓
Payment Instruments, Transactions and Electronic Archives	-	✗	Article 17	✓
CHAPTER IV FINALISATION OF PAYMENT				
<i>Section I Finalization of Payment settled through a Subsystem or Clearing House</i>				
Time of finalisation of the payment	Article 22	✓	Article 13	✓
Timeframe and responsibilities	Article 23	✓		
<i>Section II Finalisation of Payment unsettled through a Subsystem or Clearing House</i>				
Time of finalisation of the payment	Article 24	✓		
Settlement of Operations with Truncation	-	✗	Article 24	✓
CHAPTER V INFRINGEMENTS AND PENALTIES				
<i>Section I General Provisions</i>				
People Responsible / Liability of Juristic Persons, Companies and Individual Agents	Article 25	✓	Article 28	✓
Applicable Law	-	✗	Article 25	✓
Attempt and negligence	Article 26	✓		
Graduation of sanctions	Article 27	✓		
Fulfilment of omitted obligation	Article 28	✓		
<i>Section II Penal Provision</i>				
Illicit activity in the payment system	Article 29	✓		

Offences	Article 30	✓	Article 26 ⁴⁰⁰	✓
Offences of special severity	Article 31	✓		
Additional Penalties	Article 32	✓	Article 27	✓
<i>Section III Procedure</i>				
Competence and form / Institution of Proceedings and Decisions	Article 33	✓	Article 29	✓
Appeals	-	✗	Article 30	✓
Decision by order of the court	-	✗	Article 31	✓
Participation of the <i>Banco de Moçambique</i> in Proceedings	-	✗	Article 32	✓
Performance of Obligation	-	✗	Article 33	✓
Dispute / Conflict Resolution	Article 34	✓		
Consensus / Conciliation	Article 35	✓	Article 34	✓
Mediation	Article 36	✓	Article 34	✓
Arbitration	Article 37	✓	Article 35	✓
Arbitration on the Initiative of the Parties	-	✗	Article 36	✓
Arbitration in the Public Interest	-	✗	Article 37	✓
Arbitration Procedure	Article 37	✓	Article 38	✓
Deliberations of the Arbitration Commission	-	✗	Article 39	✓
Subsidiary Law	-	✗	Article 40 ⁴⁰¹	✓
CHAPTER VI FINAL AND TRANSITIONAL PROVISIONS				
Form and advertising of Central Bank's activities	Article 38	✓	-	✗
Confidentiality of Operations	Article 39	✓	-	✗
Filing obligation	Article 40	✓	-	✗
Regulations	Article 41	✓	Article 41 & 42	✓
Transitional Provision	Article 42	✓	Article 43	✓
Abrogation provision	Article 43	✓	-	✗
Doubts and omissions	Article 44	✓	-	✗
Entry into force	Article 45	✓	Article 44	✓

4.3.4 Unique Acts: Zambia's National Payment Systems Act, 2007

Zambia's National Payment Systems, 2007⁴⁰² contains several unique provisions on "payment system businesses."⁴⁰³ In terms of Section 11, the Bank of Zambia is mandated to regulate and oversee the operations of payment systems businesses to ensure the efficiency, integrity, effectiveness, competitiveness and security

⁴⁰⁰ Article 26 of Law n° No 2/2008 of 27 February covers offences and penalties.

⁴⁰¹ Article 40 of Law n° No 2/2008 of 27 February reads, "Law n° 11/99 of 12 July on arbitration, conciliation and mediation as alternative means for the resolution of conflicts shall be applicable to this Chapter in respect of any matters not specifically dealt with herein."

⁴⁰² Act 1 of 2007.

⁴⁰³ The Zambian National Payment System Act 1 of 2007 defines "payment system businesses" as, "the business of providing money transfer or transmission services or any other business that the Bank of Zambia may prescribe as a payment system business."

of the payment system so as to promote the safety and stability of the Zambian financial system. Section 12(1) requires a person intending to conduct, or offer to conduct, any payment system business to apply for designation by the Bank of Zambia. Section 13 prohibits a person from conducting a payment system business as an intermediary unless the person is, (a) a participant, (b) designated as a payment system business under section 12 or (c), exempted by the Bank of Zambia under the Act. These provisions are particularly relevant in light of the requirements set out in the BIS/World Bank *General Principles for International Remittance Services report (2007)*. Currently there are 28 designated payment system businesses in Zambia including Mobile Transactions Zambia Ltd who provide mobile payment services and money transmission services, Calltrol who provide switching services, FX Africa Bureau de Change who provide a prepaid card solution and Cactus Financial Services who provide money transmission services.⁴⁰⁴ Several banks, including Ecobank, ZANACO, Finance Bank Zambia and Stanbic Bank are also designated as payment system businesses based upon the money transmission services that they provide.

An additional feature of the Zambian National Payment Systems Act, 2007⁴⁰⁵ is the inclusion of provisions on the electronic presentment of cheques. Part IV of the National Payment Systems Act overrides the provisions in the Bills of Exchange Act, 1882 where applicable.⁴⁰⁶ Section 15(1) reads, "subject to subsection (3), a banker may present a cheque for payment to a banker, on whom it is drawn, by electronically transmitting it by other means instead of presenting the cheque itself." In terms of Section 15(2), where a cheque is presented for payment, under subsection (1), physical presentment at the premises of the drawee's bank at a reasonable hour of a working day is no longer necessary. Section 15(1) of the Zambian National Payment Systems Act, 2007 empowers the Bank of Zambia to prescribe the physical features of a cheque.

Table 27: Structure of the Zambian National Payment Systems Act, 2007

	Zambia	
	Section	
PART I PRELIMINARY		
Short title and commencement	Section 1	✓
Interpretation	Section 2	✓
Application	Section 3	✓
PART II PAYMENT SYSTEMS REGULATION		
Functions of the Bank of Zambia	Section 4	✓
Regulation, oversight and designation of payment systems	Section 5	✓
Requirements for designation	Section 6	✓
Application for designation of payment system	Section 7	✓
Existing payment systems	Section 8	✓
Directives by the Bank of Zambia	Section 9	✓
Participation of Bank of Zambia in payment systems	Section 10	✓
PART III PAYMENT SYSTEMS BUSINESS		
Regulation and oversight of payment system businesses	Section 11	✓
Designation of payment system businesses	Section 12	✓
Restriction on payment system business	Section 13	✓

⁴⁰⁴ See <http://www.boz.zm/PaymentSystems/DesignatedPaymentSystems.pdf>

⁴⁰⁵ Act 1 of 2007.

⁴⁰⁶ Article 14 of Act 1 of 2007 reads, "notwithstanding the Bills of Exchange Act, 1882, where a banker on whom a cheque is drawn has, by notice published in the Gazette, specified the address at which the cheques drawn on the banker may be presented, the cheque is presented at the proper place if it is presented at such gazetted place."

PART IV PRESENTMENT OF ELECTRONIC TRANSMISSION OF CHEQUES		
Presentment of cheque for payment	Section 14	✓
Alternative means of presentment of cheques	Section 15	✓
Admissibility of payment order	Section 16	✓
PART V SETTLEMENTS		
Validity of clearing house rules	Section 17	✓
Collateral	Section 18	✓
Suspension of participant due to inadequate collateral	Section 19	✓
Discharge of settlement obligations	Section 20	✓
Failure to settle arrangements	Section 21	✓
Application of Zambian law in certain proceedings	Section 22	✓
Winding-up of participant by court	Section 23	✓
Winding up of participant by Bank of Zambia	Section 24	✓
PART VI GENERAL ENFORCEMENT PROVISIONS		
Netting agreements	Section 25	✓
Utilisation of collateral	Section 26	✓
Returns	Section 27	✓
Retention of records	Section 28	✓
Access to information and confidentiality	Section 29	✓
Documents	Section 30	✓
False documents	Section 31	✓
Misleading names	Section 32	✓
Dishonoured cheques	Section 33	✓
Investigations	Section 34	✓
General offence and penalty and offences by body corporates	Section 35	✓
Validity of certain acts by participants	Section 36	✓
Immunity of the Bank of Zambia officials	Section 37	✓
Exemptions	Section 38	✓
Disputes between participants	Section 39	✓
Decisions of Bank of Zambia	Section 40	✓
Appeals and Appeal Tribunal	Section 41	✓
Regulations	Section 42	✓
Rules, guidelines or directives by Bank of Zambia	Section 43	✓

4.3.5 Unique Bill: Malawi’s National Payment Systems Bill

Malawi’s National Payment Systems Bill, 2014 is clearly and logically structured and contains nine parts and forty-four sections.

The powers and functions of the Reserve Bank in relation to payment, clearing and settlement systems are clearly set out in Part II. PART III is a stand-alone part on the regulation and oversight role of the Central Bank. This Bill is a good example of a “Newer Generation Act” as it’s extends well beyond the “designation or recognition of clearing and settlement systems” and the regulation and oversight thereof, as is the case in most other National Payment System Acts.

Section 3(1) of the National Payment Systems Bill, 2014 is unusual in that it states that, “the principle objective of this Act is to provide for the regulation and oversight of payment, clearing and settlement systems, payment instruments, remittance service providers, electronic money transfers, card issuers, travellers cheques agencies by –

- (a) promoting the soundness, integrity, safety and efficiency and reliability of the payment, clearing and settlement systems or payment instruments including security and operating standards, and infrastructure arrangements;
- (b) providing for minimum standards for protection of customers; and
- (c) determining respective rights and obligations of system operators, participants and customers.”

This Section extends the ambit of the regulation and oversight of the Reserve Bank from simply looking at SIPS into the retail payments domain.

Additionally, Section 12(1) prohibits a person from establishing or operating any payment, clearing and settlement system or services, remittance services including electronic money transfer services, mobile payment services or issuing payment instruments without a licence or prior authorisation from the Reserve Bank from the Reserve Bank of Malawi.

The structure of the National Payment Systems Bill, 2014 is set out in Table 28 below.

Table 28: Structure of the Malawian National Payment Systems Bill, 2014

	Malawi	
	Section	
PART I: PRELIMINARY		
Short title and commencement	Section 1	●
Interpretation	Section 2	●
Objectives	Section 3	●
PART II: POWERS AND FUNCTIONS OF THE RESERVE BANK IN RELATION TO PAYMENT, CLEARING AND SETTLEMENT SYSTEMS		
Powers of the Reserve Bank	Section 4	●
Delegation of powers not to preclude exercise of delegated powers by the Reserve Bank	Section 5	●
Limitation on powers to delegate	Section 6	●
Cooperation with other regulatory authorities	Section 7	●
Directives and guidelines	Section 8	●
Breach of directives, etc	Section 9	●
Court order for compelling compliance with a direction	Section 11	●
PART III: REGULATION AND OVERSIGHT BY THE RESERVE BANK		
Restriction on operating payment system, etc. or services	Section 12	●
Application for licence or authorisation	Section 13	●
License and authorisation requirements	Section 14	●
Revocation or suspension of authorization or a license	Section 15	●

Responsibilities of system operators	Section 16	●
Actions requiring prior approval of the Reserve Bank	Section 17	●
Investigative powers of the Reserve Bank	Section 18	●
Requirements for participation in, and operation of, a settlement system	Section 19	●
PART IV: PROTECTION OF SETTLEMENT SYSTEMS		
Discharge of settlement obligations	Section 20	●
Finality and irrevocability of settlement	Section 21	●
Winding up of settlement system participant on application by any person other than the Reserve Bank	Section 22	●
Winding up of settlement system participant by the Registrar	Section 23	●
Voluntary winding up of a settlement system participant	Section 24	●
Irrevocability and finality of settlements prior to lodgement of winding-up order	Section 25	●
Cessation of participation in payment systems	Section 26	●
Passing of settlement transactions subsequent to insolvency proceedings	Section 27	●
Restrictions against attachments, garnishee proceedings or seizures	Section 28	●
PART V: NETTING AND FINANCIAL COLLATERAL ARRANGEMENTS		
Obligations under netting agreements, arrangements and rules	Section 29	●
Recognition of financial collateral arrangements	Section 30	●
Utilisation of collateral	Section 31	●
PART VI: TRUNCATION, IMAGING AND ELECTRONIC ENTRIES		
Truncation and imaging	Section 32	●
Admissibility of photographic images of payment instruments and electronic entries	Section 33	●
Right of a bank to request original payment instrument or image thereof	Section 34	●
PART VII: DISPUTE RESOLUTION		
Dispute resolution	Section 35	●
PART VIII: MISCELLANEOUS		
Access to information	Section 36	●
Confidentiality of information	Section 37	●
Use of confidential information for personal gain	Section 38	●
Condition for disclosure of information	Section 39	●
Indemnity of officers and other officials	Section 40	●
Retention of records	Section 41	●
Penalties	Section 42	●
Regulations	Section 43	●
PART IX: TRANSITIONAL ARRANGEMENTS		
Transitional arrangements	Section 44	●

4.3.6 Unique Draft Act: The DRC's Draft Law on the Provisions Applicable to the National Payment System

The DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 is particularly unique in that, it is the longest Act in the region (108 Articles), the articles do not have headings (the headings in Table 29 below have been inserted based upon an interpretation of the text), contains detailed provisions on payment instruments, access to financial services, interoperability, payment instruments, the obligations of payment service providers, issuer obligations, holder obligations, E-Money, evidence and electronic signatures and the monitoring of payment systems and payment instruments. The DRC's Draft Law on the Provisions

Applicable to the National Payment System, 2013 appears to incorporate several provisions from Directive 2007/64/EC Payment Services in the Internal Market (PSD) and combine these with provisions found in “conventional” National Payment System Acts.

Table 29: Structure of the DRC’s Draft Law on the Provisions Applicable to the National Payment System

	DRC	
	Article	
TITLE I: OBJECT, SCOPE AND DEFINITIONS		
CHAPTER I: OBJECT AND SCOPE		
Purpose of the Act	Article 1	●
Application of the Act	Article 2	●
CHAPTER II: DEFINITIONS		
Definitions	Article 3	●
TITLE II: PROVISIONS REGARDING PAYMENT SYSTEMS		
CHAPTER I: FUNCTIONING RULES OF THE PAYMENT SYSTEMS		
Functioning Rules to be developed by Participants	Article 4	●
Scope of Functioning Rules	Article 5	●
CHAPTER II: PROTECTION OF THE PAYMENT SYSTEM		
SECTION I: IRREVOCABILITY OF PAYMENTS AND SETTLEMENTS		
Irrevocability of Payments and Settlements	Article 6	●
Transfer Orders	Article 7	●
Insolvency Proceedings	Article 8	●
Duty to Inform the Central Bank of Insolvency Proceedings	Article 9	●
Seizing and Impounding of Settlement Account Balance	Article 10	●
Insolvency of a Foreign Participant	Article 11	●
SECTION III: FINANCIAL COLLATERAL		
Suitable Financial Collateral	Article 12	●
Financial Collateral Valid and Binding of Third Parties	Article 13	●
Close-out Netting Provisions Valid and Binding on Third Parties	Article 14	●
Financial Collateral Agreement	Article 15	●
Enforcement Event	Article 16	●
Collateral Cannot be Declared Void or be Revoked due to Opening of Insolvency Proceedings	Article 17	●
Applicable Law	Article 18	●
TITLE III: PROVISIONS REGARDING PAYMENT INSTRUMENTS		
CHAPTER I: GENERAL PROVISIONS		
SECTION I: USING PAYMENT INSTRUMENTS		
Obligation to Provide a Contract	Article 19	●
Provisions of the Contract	Article 20	●
Signature of Drawer	Article 21	●
Written Proof	Article 22	●
SECTION II: OBJECTIONS TO PAYMENTS		
Situations in Which Objections Can Be Made	Article 23	●
Revocation	Article 24	●
Un-Authorised or Defective Transactions	Article 25	●

Conditions for Re-imbusement of Funds	Article 26	●
Non-Execution as Result of Instructing Party	Article 27	●
Payment Period for Delivery	Article 28	●
CHAPTER II: PROMOTING PAYMENT INSTRUMENTS		
SECTION I: ACCESS TO FINANCIAL SERVICES		
Right to Open an Account	Article 29	●
Minimum Banking Services	Article 30	●
Payments to be Electronic or by Cheque	Article 31	●
Information and Awareness Raising	Article 32	●
SECTION II: INTERBANKING AND INTEROPERABILITY		
Central Bank to Set Terms and Conditions	Article 33	●
CHAPTER III: TRANSFER		
Content of Transfer Orders	Article 34	●
Irrevocability	Article 35	●
Date of Acceptance of Transfer Order	Article 36	●
Full Amount	Article 37	●
Public Disclose of Terms and Conditions and Price Lists	Article 38	●
CHAPTER IV: DRAWDOWNS		
Drawdown Order Notice and Transfer	Article 39	●
Non Irrevocability	Article 40	●
Duty to Inform the Debtor of Levies	Article 41	●
Drawdown Results in Transfer	Article 42	●
Principles of Drawdowns to be set by the Central Bank	Article 43	●
Rejection of Drawdown	Article 44	●
CHAPTER V: BANK CARD, OTHER INSTRUMENTS AND ELECTRONIC FUND TRANSFER PROCESS		
SECTION I: ISSUER'S OBLIGATIONS		
Contract and Contractual Conditions	Article 45	●
Issuer Liability	Article 46	●
Cancellation of Card	Article 47	●
Authorisation of Automatic Debit Order	Article 48	●
Un-authorised Transactions	Article 49	●
SECTION II: SERVICE PROVIDER OBLIGATIONS		
Service Provider Obligations	Article 50	●
SECTION III: HOLDERS OBLIGATIONS		
Holders Obligations in the Event of Loss or Theft of Card	Article 51	●
Holders Liability	Article 52	●
Refund of Disputed Amounts	Article 53	●
Holders Obligations	Article 54	●
Duty to Inform the Issuer of Unauthorised Transactions and Errors	Article 55	●
CHAPTER VI: E-MONEY		
Central Bank States Terms and Conditions for Issuance of E-Money	Article 56	●
Definition of E-Money	Article 57	●
Limitations on the Issuance of E-Money	Article 58	●
TITLE IV: MONITORING PAYMENT SYSTEMS AND PAYMENT INSTRUMENTS		
Monitoring by Central Bank	Article 59	●
Application and Approval to Issue Payment Instrument	Article 60	●
Access to Information, Documentation, Inspections and Audits	Article 61	●

TITLE V: EVIDENCE AND ELECTRONIC SIGNATURES		
Electronic Transactions Constitute Proof and are Legally Admissible	Article 62	●
Documentary Evidence	Article 63	●
Electronic Signatures	Article 64	●
Electronic Signatures Accepted as Evidence	Article 65	●
Approval of Certification Systems by the Central Bank	Article 66	●
TITLE VI: PREVENTION AND CENTRALISATION OF PAYMENT INCIDENTS		
CHAPTER I: PAYMENT INCIDENTS CENTRAL		
Organisation and Management of <i>Payment Incidents Central</i>	Article 67	●
Access to Information Contained in the of <i>Payment Incidents Central</i> Files	Article 68	●
Retention of Records	Article 69	●
CHAPTER II: OBLIGATIONS OF PAYMENT INSTRUMENT ISSUERS		
Obligations of Payment Instrument Issuers	Article 70	●
CHAPTER III: DRAWEE'S OBLIGATIONS		
Declaration of Incidents and Other Obligations	Article 71	●
Unpaid Payment Instrument Issued by a Trustee	Article 72	●
Joint Account Holders	Article 73	●
CHAPTER IV: WARNING, REGULARISATION, BAN IMPOSED BY THE BANK		
SECTION I: WARNING		
Warning Letters	Article 74	●
Regularisation	Article 75	●
REGULARISATION		
Liability for a Penalty in the Event of Failure to Regularise Account	Article 76	●
Proportionality of Penalty	Article 77	●
SECTION III: BAN IMPOSED BY THE BANK		
Ban on the Issuance of Payment Instruments	Article 78	●
Right to Lodge an Action for Annulment	Article 79	●
Central Bank to Set Terms and Conditions for Proceedings	Article 80	●
CHAPTER V: LEGAL RESTRICTION		
Legal Restrictions Pronounced on an Individual Basis	Article 81	●
Sanctions Against Banned User who Issues a Payment Instrument	Article 82	●
Co-perpetrators	Article 83	●
Period of the Ban	Article 84	●
CHAPTER VI: OBLIGATIONS AND JURISDICTION PUBLIC PROSECUTOR'S OFFICE		
Duty of the Jurisdictions and Public Prosecutor's Office	Article 85	●
Duty of Central Bank to Inform Competent Jurisdictions / Authorities	Article 86	●
TITLE VII: COERCIVE MATTERS		
CHAPTER I: DISCIPLINARY AND ADMINISTRATIVE SANCTIONS		
Available Remedies	Article 87	●
Power to Issue a Directive and Levy Administrative Fine	Article 88	●
Proceeds of Administrative Fine	Article 89	●
CHAPTER II: PENAL SANCTIONS		
SECTION I: OFFENCES AND SENTENCES SPECIFIC TO PAYMENT OR AUTOMATED DATA PROCESSING SYSTEMS		
Articles 90 to 94	Article 90 - 94	●
SECTION II: OFFENCES AND SENTENCES SPECIFIC TO BANK CARDS, PAYMENT INSTRUMENTS AND		

ELECTRONIC PAYMENT PROCESSING		
Articles 95 to 99	Article 95 - 99	●
SECTION III: OFFENCES AND SENTENCES RELATED TO CHEQUES AND OTHER INSTRUMENTS DRAWN-OUT WITHOUT IN RIGHTS		
Article 100	Article 100	●
SECTION IV: OFFENCES SPECIFIC TO PARTICIPANTS IN PAYMENT SYSTEMS		
Articles 101 - 104	Article 101 - 104	●
TITLE VIII: VARIOUS AND FINAL PROVISIONS		
Articles 105 to 108	Article 105 - 108	●

Mauritius is the only country in the SADC that has elected not to enact a National Payment System / Payment System Management Act. As is indicated throughout this report, the fact that Mauritius does not have a legally enforceable National Payment System Act and is not in the process of drafting a Bill is of considerable concern. It is highly recommended that Mauritius reconsider their policy stance on this matter as the lack of an National Payment System Act leads to legal uncertainty and may result in private sector operators and payment service providers being unchecked and free to do as they chose.

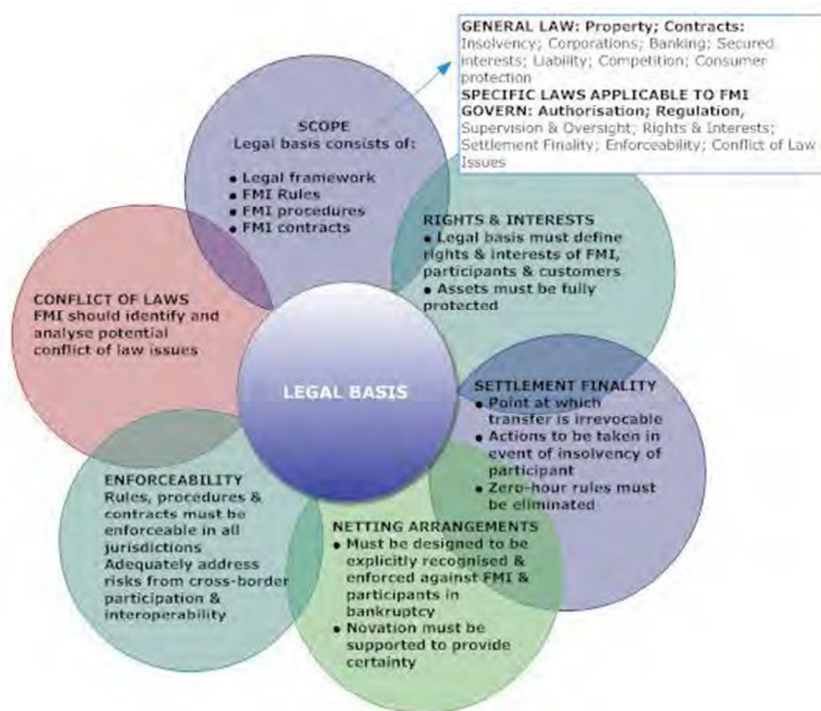
SECTION 5: REVIEW OF EACH MEMBER STATE'S PRIMARY PAYMENT STATUTE

This section of the report reviews the substantive content of the primary payments statute applicable in each SADC Member State. Two distinct approaches have been adopted for this purpose. The first approach adopted is that of a comparative review. The provisions found in each Act covering 1) definitions; 2) public interest objectives; 3) the powers, functions, regulations and oversight by the Central Bank; 4) the provisions covering confidentiality, disclosure of information and indemnity of officers and persons employed by the Central Bank; 5) the prohibition against payment intermediation; 6) conflict of laws; and 7) dispute resolution are evaluated by comparing one country's statute with another in order to identify the content of the law and any substantial gaps.

Provisions on 1) settlement finality and irrevocability; 2) transfer orders and netting; 3) provisions concerning insolvency and 4) collateral security are compared to the international best practice benchmark chosen for this exercise, namely Directive 98/26/EC Settlement Finality in Payment and Securities Settlement Systems.

Wherever practicable, the provisions found in each SADC Member States domestic National Payment System Act are measured against the PFMI Principles. Diagram 10 presents a schematic representation of the key issues noted in the Explanatory Notes of the PFMI report.

Diagram 10: Scope of a “Sound Legal Basis”



It is particularly important to note that the PFMI Report highlights the importance of the legal basis clearly:

- 1) Defining the rights and interests of FMI;
- 2) The need for a clear basis regarding when settlement finality occurs
- 3) The importance of the enforceability of netting arrangements having a sound and transparent legal basis
- 4) The enforceability of rules, procedures and contracts of FMIs in operation being enforceable in all relevant jurisdictions and;
- 5) Appropriate conflict of law provisions.

5.1 Definitions

A section containing definitions of various words or phrases used in an Act and or Subsidiary Legislation (Regulations, Determinations, and Directives) is usually near the beginning of the Act. The headings of such sections vary. Some SADC countries use the word 'Interpretation'⁴⁰⁷, others 'Definitions'⁴⁰⁸, others 'Terms used'. Occasionally, as is the case in the Mozambican Law n° 2/2008 of 27 February, definitions are contained in a 'Glossary' at the back of an Act.⁴⁰⁹ On several occasions during the research phase of this project, the need for a common understanding of key payment related terms by SADC Regulators has been raised. The lack of consensus leads to legal uncertainty and general confusion when, for example, terms such as E-Money have vastly different meanings in each SADC Member State. This problem has been resolved in the EU through the passing of Regulations and Directives, passed either jointly by the EU Council and European Parliament, or by the Commission alone that contain set definitions which are adopted automatically by Member States in the case of Regulations and incorporated into domestic laws and regulations by Member States in the case of Directives.

⁴⁰⁷ Interpretation is used by Botswana, Lesotho, Malawi, Seychelles, Zambia and Zimbabwe.

⁴⁰⁸ Definitions are used by Angola, the DRC, Namibia and South Africa.

⁴⁰⁹ A Glossary is used by Mozambique.

5.1.1 Comparative Review (Definitions in Domestic Law)

Table 30 below lists all of the terms defined in all 14 SADC Member States National Payment System Act / Bill or Payment System Management Act / Bill and Subordinate Legislation. As Mauritius does not have an National Payment System Act or Bill, and Tanzania's Bill is not available for public comment, the terms defined in the Central Bank Act, RTGS and Clearing House Rules are marked with a (*) and not included in the count in the far right hand column as this analysis focuses on the National Payment System Act / Bill and Subordinate Legislation. Provisions found in Guidelines and Guidance Notes are also not included in the count in the far right hand column.

Table 30: Key Definitions Contained in National Payment System Act and Subsidiary Legislation (Regulations / Determinations)

	Definition	ANG	BW	DRC	L50	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No. 410
A. Key Definitions Contains in National Payment System Acts & Subsidiary Legislation (SADC)																
1	Access	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	2
2	Acceptor	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
3	Agent	✗	✗	✓	●	✗	✗	✗	✓	✗	✗	✗	●	✗	✗	3
4	Agent Accounts	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	1
5	Bank(s) / Banking Institution	✗	✗	✗	●	●	*	✓	✓	✗	✓	✓	*	✓	✗	7
6	Banks Act	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	2
7	Beneficiary Bank	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	1
8	Beneficiary Service Provider	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	1
9	Bilateral Netting	✗	✓	✗	●	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	3
10	Body / Payment System Management Body	✗	✗	✗	●	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	3
11	Book Entry System	✗	✗	✗	●	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
12	Book Entry Securities Collateral	✗	✗	✗	●	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
13	Branch of a Foreign Institution	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	1
14	Business Day	✗	✗	✗	✗	●	✗	✗	✓	✗	✗	✗	✗	✗	✗	2
15	Card	✗	✗	✗	✗	●	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
16	Cash	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0
17	Central Bank or Reserve Bank	✓	✓	●	●	●	*	✗	✓	✓	✓	✓	✗	✓	✓	11
18	Central Bank Money	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0
19	Central Bank Settlement System	✗	✓	✗	●	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	5
20	Central Bank Settlement System Participant	✗	✗	✗	●	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	2
21	Central Counter Party	✗	✗	●	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	2
22	Cheque	✗	✗	✗	✗	●	✗	✗	✓	✗	*	✗	✗	✓	✗	3
23	Clear or Clearing	✗	✓	✗	●	●	*	✗	✓	✓	✓	✓	✗	✓	✓	9
24	Clearance (Clearing) and Settlement System	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	4
25	Clearance and Settlement System Operator	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
26	Clearing System Participant	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	1
27	Clearing Bank	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
28	Clearing System / Clearing House / Clearing House	✓	✓	✗	●	●	*	✓	✓	✗	✓	✓	*	✓	✓	10
29	Clearing House Operator / PCH System Operator	✗	✗	✗	●	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	2

⁴¹⁰ Number of countries defining the term.

30	Clearing House Rules	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
31	Clearing, Netting and Settlement Agreements	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	1
32	Closed-loop or Private Label System	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
33	Close-out Netting Provision	x	x	●	●	x	x	x	x	x	x	x	x	x	x	x	2
34	Collateral / Acceptable Collateral	x	✓	x	●	x	x	x	x	x	x	x	x	✓	x	x	3
35	Collateral Provider	x	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
36	Collateral Taker	x	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
37	Commencement of winding	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
38	Companies Act	x	x	x	x	x	x	✓	✓	✓	x	x	x	x	x	x	3
39	Credit Card	x	x	●	x	x	x	✓	✓	x	x	x	●	x	x	x	3
40	Credit Transfer	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
41	Cross Border Merchant Acquiring	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
42	Debit Authorisation	x	x	●	x	x	x	x	x	x	x	x	x	x	x	x	1
43	Debit Card	x	x	x	x	x	x	✓	✓	x	x	x	●	x	x	x	2
44	Debit Transfer	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
45	Designate	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
46	Designated Clearing System Participant	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
47	Designated Non-Bank Financial Institution (NBFI)	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
48	Designated Payment System	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
49	Designated Settlement System	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
50	Designated Settlement System Operator	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
51	Designated Settlement System Participant	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
52	Direct Participant	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
53	Document	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
54	Domestic Card Transactions	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
55	Domestic Interbank Card Transactions	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
56	Domestic Merchant Acquirer	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
57	Duty to Settle	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1
58	Electronic Funds Transfer	x	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
59	Electronic Instrument	x	x	●	x	x	x	x	x	x	x	x	x	x	x	x	1
60	Electronic Medium	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
61	Electronic Money	x	x	✓	x	x	x	*	✓	x	●	✓	●	x	x	x	4
62	Electronic Money Institution	x	x	✓	x	x	x	*	x	x	x	x	x	x	x	x	1
63	Electronic Money Issuer	x	x	●	x	x	x	✓	x	x	x	x	x	x	x	x	2
64	Electronic Payment Scheme	x	x	x	x	x	x	x	x	x	✓	●	x	x	x	x	1
65	E-Money Scheme	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	1

66	Electronic Transactions	x	x	x	x	x	x	✓	●	x	x	x	x	x	x	2
67	Electronic Transmission	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
68	Enforcement Event	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
69	Failure to Settle	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
70	Failure to Settle Arrangements	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
71	Finalisation of Payment / Payment Finality	✓	x	x	x	●	x	✓	x	x	x	x	●	✓	x	4
72	Financial Collateral	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
73	Financial Collateral Arrangement	x	x	x	●	●	x	x	x	x	x	x	x	x	x	2
74	Financial Institution	x	✓	x	●	x	x	x	x	x	✓	x	✓	✓	x	5
75	Financial Instrument(s)	x	x	●	●	x	x	x	x	✓	x	x	x	x	x	3
76	Float	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
77	Foreign or International Merchant Acquirer	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
78	Funds	x	✓	x	x	x	x	x	✓	x	✓	x	x	x	x	3
79	Gross Settlement	x	✓	x	x	x	x	x	x	x	✓	x	x	x	x	2
80	Guarantee / Financial Guarantee	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
81	Holding Company	x	x	x	x	●	x	x	✓	x	x	x	x	x	x	2
82	Information & Communication Technologies	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
83	Insolvency Act / Bankruptcy and Insolvency Act	x	x	x	x	x	x	✓	✓	x	x	x	x	x	x	2
84	Insolvency Proceedings	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
85	Interoperability	x	x	x	x	x	x	✓	x	●	✓	● 411	x	x	x	3
86	Issuer of a Payment Instrument	x	x	●	x	x	x	✓	x	x	x	x	x	x	x	2
87	Indirect Participant	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
88	Intra-day Liquidity	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
89	Intra-day Settlement	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
90	Inter-bank Payment System	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
91	Intermediary	x	x	x	x	x	x	x	x	x	x	x	✓	✓	x	2
92	Irrevocable	x	x	x	x	x	x	x	x	x	x	x	✓	✓	x	2
93	Management Body	x	✓	x	x	x	x	✓	✓	x	✓	x	x	x	x	4
94	Master Agreement	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
95	Merchant	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
96	Merchant Acquirer	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
97	Method of Payment	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
98	Mobile Payment System	x	x	x	x	●	x	x	x	x	x	x	x	x	x	1
99	Money	x	x	x	x	x	x	✓	x	✓	x	x	✓	✓	x	4
100	Multilateral Clearing	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1

⁴¹¹ Interoperability is defined in the Electronic Payment Scheme Guidelines, 2007.

101	Multilateral Netting	x	✓	●	●	x	x	x	x	✓	x	✓	x	x	x	5
102	National Payment System	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
103	National Payment System Coordinating Committee	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
104	Netting	x	✓	●	●	●	*	x	✓	✓	✓	✓	x	✓	✓	10
105	Netting Arrangement	x	x	x	●	x	x	x	x	x	x	x	x	✓	✓	3
106	Netted Balance	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
107	Notify	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
108	Obligation / Payment Obligation	x	✓	x	x	x	x	x	✓	✓	✓	✓	x	✓	✓	7
109	Off-us Transactions	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
110	On-us Transactions	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
111	Open-loop System	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
112	Operator	✓	x	x	●	x	x	✓	x	x	x	x	x	x	x	3
113	Outstanding Electronic Money Liabilities	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
114	Oversight	✓	x	x	x	●	x	✓	x	x	x	✓	x	x	x	4
115	Participant	✓	x	●	●	x	*	✓	x	✓	x	x	✓	✓	✓	8
116	Player / Stakeholder	✓	x	x	x	x	x	✓	x	x	x	x	x	x	x	2
117	Payer Service Provider	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	1
118	Paying Bank	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
119	Payment	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	1
120	Payment Card	x	x	x	●	x	x	✓	x	x	x	x	x	x	x	2
121	Payment Instruction	✓	x	x	x	●	x	✓	✓	✓	x	x	*	✓	✓	5
122	Payment Institution	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
123	Payment Instrument	x	x	●	●	●	x	x	✓	✓	✓	✓	x	x	x	7
124	Payment Operation	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	1
125	Payment Order	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
126	Payment Service	✓	x	x	x	x	x	✓	✓	x	x	x	x	x	x	3
127	Payment System	✓	x	●	●	●	x	x	✓	x	✓	x	*	✓	✓	8
128	Payment System Arrangement	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
129	Payment System Business	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
130	Payment System Services	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
131	Payment Scheme	x	x	x	x	x	x	x	x	x	x	x	●	x	x	1
132	Payment Service Provider	✓	x	x	x	x	x	✓	✓	x	x	x	x	x	x	3
133	Person	x	x	x	x	●	x	x	x	x	✓	x	x	✓	✓	4
134	Payment Subsystem	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	1
135	Pre-paid Product / Card	x	x	x	x	x	x	✓	✓	x	x	x	x	x	x	2
136	Promoter	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
137	Realisation of Collateral	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
138	Real-time Transactions	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
139	Receiving Bank	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
140	Recognised System	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	x	3
141	Relevant Account	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1

142	Remittance	x	x	x	x	o	x	x	x	o	x	x	x	x	x	2
143	Remittance Service Provider	x	x	x	x	o	x	x	x	o	x	x	x	x	x	2
144	Securities	✓	x	x	x	x	*	✓	x	✓	x	x	x	x	x	3
145	Securities Settlement System	x	x	x	o	x	x	x	x	x	x	x	x	x	x	1
146	Settlement	x	✓	x	o	o	x	x	✓	✓	✓	✓	*	✓	✓	9
147	Settlement Account	✓	x	o	o	o	x	✓	✓	x	x	x	x	x	x	6
148	Settlement Agent	x	x	o	o	o	x	x	x	x	x	x	x	✓	✓	5
149	Settlement Asset	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	1
150	Settlement Cycle	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	2
151	Settlement Finality or Final Settlement	✓	x	x	x	x	x	✓	x	x	x	x	o	✓	✓	5
152	Settlement Instruction	✓	x	x	o	o	x	✓	✓	x	✓	x	x	x	x	6
153	Settlement Obligation	✓	x	x	x	o	x	x	x	x	✓	x	x	✓	✓	5
154	Settlement of Securities	✓	x	x	x	x	x	✓	x	x	x	x	x	x	x	2
155	Settlement System	x	✓	x	x	o	x	x	✓	✓	✓	✓	*	x	x	6
156	Settlement System Participant	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	1
157	Skimming Device	x	x	x	o	x	x	x	x	x	x	x	x	x	x	1
158	Sorting at Source	x	x	x	x	x	x	x	✓	x	✓	x	x	x	x	2
159	Subsidiary	x	x	x	x	o	x	x	✓	x	x	x	x	x	x	2
160	Subsystem	✓	x	x	x	x	x	✓	x	x	x	x	x	x	x	2
161	System	x	x	x	o	x	x	x	x	✓	x	✓	x	x	x	3
162	System Operator	x	x	o	x	o	x	x	x	x	✓	x	x	x	x	3
163	System Participant	x	x	x	x	o	x	x	✓	✓	x	x	x	x	x	3
164	Systemic Risk	x	✓	x	o	o	x	x	✓	✓	✓	✓	o	✓	✓	9
165	Title Transfer Arrangement	x	x	x	o	x	x	x	x	x	x	x	x	x	x	1
166	Transfer	x	✓	o	x	x	x	x	x	✓	x	✓	x	x	x	4
167	Transfer Order / Transfer Instruction	x	✓	x	o	o	x	x	x	✓	x	✓	x	x	x	5
168	Truncation	x	x	x	o	o	x	✓	x	x	x	x	x	x	x	3
169	Users	✓	x	o	x	x	x	✓	x	x	x	x	x	x	x	3
170	Winding-up Proceedings	x	x	x	x	o	x	x	x	x	x	x	x	x	x	1

5.1.2 Measurement of Terms in Domestic Legislation against International Best Practice (EU Directives)

Sixteen terms are defined in Directive 98/26/EC Settlement Finality in Payment and Securities Settlement Systems. As represented in Table 31 below, of these sixteen essential terms, two are not found in any Act or Regulation in force in a SADC Member State.

Table 31: Terms Defined in the Settlement Finality Directive 98/26/EC

Term	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No. ⁴¹²
Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC)															
System	x	x	x	o	x	x	x	x	✓	x	✓	x	x	x	3
Institution	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Central Counterparty	x	x	o	x	x	x	✓	x	x	x	x	x	x	x	2
Settlement Agent	x	x	o	o	o	x	x	x	x	x	x	x	✓	x	4
Clearing House	✓	✓	x	o	o	x	✓	✓	x	✓	✓	✓	✓	✓	11
Participant	✓	x	o	o	x	x	✓	x	✓	x	x	✓	✓	x	7
Indirect Participant	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Securities	✓	x	x	x	x	x	✓	x	✓	x	x	x	x	x	3
Transfer Order	x	✓	x	o	o	x	x	x	✓	x	✓	x	x	x	5
Insolvency Proceedings	x	x	x	o	o	x	x	x	x	x	x	x	x	x	2
Netting	x	✓	o	o	o	x	x	✓	✓	✓	✓	x	✓	✓	10
Settlement Account	✓	x	o	o	x	x	✓	✓	x	x	x	x	x	x	5
Collateral Security	x	✓	x	o	x	x	x	x	x	x	x	x	✓	x	3
Business Day	x	x	x	x	o	x	x	x	x	x	x	✓	x	x	2
Interoperable System	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
System Operator	x	x	o	x	o	x	x	x	x	✓	x	x	x	x	3

The four essential terms defined in Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions are electronic money institution⁴¹³, electronic money⁴¹⁴, electronic money issuer⁴¹⁵ and Average Outstanding Electronic Money.⁴¹⁶ As represented in Table 33 below, very few SADC Member States define all of these terms.

⁴¹² Number of countries defining the term.

⁴¹³ See Article 2.1 Directive 2009/110/EC. "Electronic Money Institution" is defined as, "a legal person that has been granted authorisation under Title II to issue electronic money."

⁴¹⁴ See Article 2.2 Directive 2009/110/EC. "Electronic Money" is defined as, "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer (Article 2.2)"

⁴¹⁵ See Article 2.3 Directive 2009/110/EC. "Electronic Money Issuers" are defined as, "entities referred to in Article 1(1), institutions benefiting from the waiver under Article 1(3) and legal persons benefiting from a waiver under Article 9)."

⁴¹⁶ See Article 2.4 Directive 2009/110/EC. "Average Outstanding Electronic Money" is defined as, "average outstanding electronic money' means the average total amount of financial liabilities related to electronic money in issue at the end of each calendar day over the preceding six calendar months, calculated on the first calendar day of each calendar month and applied for that calendar month."

Table 32: Terms Defined in Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions

Term	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No.
Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions															
Electronic Money Institution	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	1
Electronic Money	x	x	✓	x	x	x	x	✓	x	●	✓	●	x	x	5
Electronic Money Issuer	x	x	●	x	x	x	x	✓	x	x	x	x	x	x	2
Average Outstanding Electronic Money	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0

When the terms defined in domestic National Payment System Law and Regulation are compared against the terms defined in Directive 2007/64/EC Payment Services in the Internal Market (PSD) the situation is even worse. Of the thirty terms defined in Directive 2007/64/EC only ten are defined by any SADC Member State. It is important to note that basis terms such as payer, payee, framework contract, money remittance, value date, authentication and unique identifier are not defined by a single SADC Member State.

Table 33: Terms Defined in Directive 2007/64/EC Payment Services in the Internal Market (PSD)

Term	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No.
Directive 2007/64/EC Payment Services in the Internal Market (PSD)															
Home Member State	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Host Member State	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Service	✓	x	x	x	x	x	✓	✓	x	x	x	x	x	x	3
Payment Institution	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Payment Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment System	✓	x	●	●	●	x	x	✓	x	✓	x	*	✓	x	7
Payer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Service Provider	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	1
Payment Service User	✓	x	●	x	x	x	✓	x	x	x	x	x	x	x	3
Consumer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Framework Contract	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Money Remittance	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Account	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Funds	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	x	3
Payment Order	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Value Date	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Reference Exchange Rate	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Authentication	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Reference Interest Rate	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Unique Identifier	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0

Agent	x	x	✓	●	x	x	x	✓	x	x	x	x	x	x	3
Payment Instrument	x	x	●	●	x	x	x	✓	✓	✓	✓	x	x	x	6
Means of Distance Communication	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Durable Medium	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Micro-enterprise	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Business Day	x	x	x	x	●	x	x	✓	x	x	x	x	x	x	2
Direct Debit	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Branch	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	1
Group	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0

5.1.3 Measurement against International Best Practice (The EU Regulations)

As noted in section 3.2.1 of this report, the first Regulation adopted by the EU in the payments space was Regulation (EC) No 2560/2001 on Cross-border Payments in Euro, adopted in 2001. This Directive is said to have “laid the foundations of its Single Euro Payments Area (SEPA) policy through former Regulation 2560/2001 on cross-border payments in euro, whereby banks are not permitted to impose different charges for domestic and cross-border payments or ATM withdrawals in the EU-27. Regulation 2560/2001 has also generally been understood as a turning point in the financial integration policy of the European legislator: beyond its formal stipulations, the Regulation at the time of its inception was clearly intended to shock the banking sector into stepping up its efforts to achieve the Single Euro Payments Area (SEPA).”⁴²⁷ The revised version of this Regulation, Regulation (EC) No 924/2009 on Cross-border Payments in the Community was approved by the European Parliament on 24 April 2009.

Tables 34 and 35 below provides a summary of the key terms defined in Regulation (EC) No 924/2009 Cross-border Payments in the Community and Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro. As is to be expected, given the fact that there is currently no SADC wide legal and regulatory framework in place for cross-border payments, most of the terms defined in Regulation (EC) No 924/2009 are not defined by SADC Member States in their domestic National Payment System Act or subordinate legislation.

Table 34: Terms Defined in Regulation (EC) No 924/2009 Cross-border Payments in the Community

Definition	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No.
Regulation (EC) No 924/2009 Cross-border Payments in the Community															

⁴²⁷ See European Payments Council (EPC) AISBL *Making SEPA a Reality - The Definitive Guide to the Single Euro Payments Area* where it is noted further that, “the revised version of this Regulation approved by the European Parliament on 24 April 2009 introduces additional provisions which - in the eyes of the regulator - further promote EU financial integration in general and SEPA implementation in particular. The revised Regulation has significant impact due to the introduction of the following provisions: (1) the price parity requirements are extended to direct debits; (2) the setting out of clear rules for transaction-based multilateral interchange fees until November 2012; (3) banks in the euro area offering direct debits today in euro to debtors are mandated to become reachable for SEPA Direct Debit collections from November 2010 onwards. The revised Regulation - now labelled Regulation on cross-border payments in euro in the Community - will be applicable in all Member States from 1 November 2009 onwards.”

Cross-border Payment	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
National Payment	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Service Provider	✓	x	x	x	x	x	✓	✓	x	✓	x	x	x	x	4
Payment Service User	✓	x	●	x	x	x	✓	x	x	x	x	x	x	x	3
Payment Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Order	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	1
Charge	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Funds	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	x	3
Consumer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Micro-enterprise	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Interchange Fee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Direct Debit	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0

Table 35: Terms Defined in Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro

Definition	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	No. ⁴¹⁸
Regulation (EU) No 260/2012 Technical and Business Requirements for Credit Transfers and Direct Debits in Euro															
Credit Transfer	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Direct Debit	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Account	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment System	✓	x	●	●	●	x	x	✓	x	✓	x	●	✓	x	8
Payment Scheme	x	x	x	x	x	x	x	x	x	x	x	●	x	x	1
Payment Service Provider	✓	x	x	x	x	x	✓	✓	x	x	x	x	x	x	3
Payment Service User	✓	x	●	x	x	x	✓	x	x	x	x	x	x	x	3
Payment Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Payment Order	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Interchange Fee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
MIF	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
BBAN	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
IBAN	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
BIC	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
ISO 20022 XML Standard	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Large-value Payment System	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Settlement Date	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0
Collection	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0

⁴¹⁸ Number of countries defining the term.

Mandate	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
Retail Payment System	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
Micro-enterprise	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
Consumer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
R-Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
Cross-Border Payment Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
National Payment Transaction	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o
Reference Party	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	o

5.2 The Role of the Central Bank in the National Payment System

Kokkola notes that, “in payment, clearing and settlement systems, central banks aim mainly to: (i) prevent systemic risk, thereby maintaining financial stability; (ii) promote the efficiency of payment systems and instruments; (iii) ensure the security of the public trust in the currency as the settlement asset; and (iv) safeguard the transmission channel for monetary policy.”⁴¹⁹ To fulfill these objectives, the Central Bank typically acts in a variety of capacities. These are 1) as the operator or provider of payment services, 2) as a catalyst by drafting legislation and regulations and issuing directives and guidelines, 3) as the Oversight Authority and 4) as a user of payment services in its operational activities.

Taking these potential roles into consideration, with particular emphasis on the oversight authority role of the Central Bank, in the section that follows, provisions found in the Central Bank Act and the National Payment System Act, specifically pertaining to the powers, functions and regulatory and oversight role mandated to the Central Bank with respect to the National Payment System are compared. The objective of this exercise is to benchmark provisions and to assess whether there are any potential gaps in each Act which the Central Bank should consider rectifying by either amending the primary National Payment System Act / Bill or issuing subordinate regulations / determinations under the current Act, should one have been promulgated.

5.2.1 Powers, Functions, Regulation and Oversight by the Central Bank

5.2.1.1 Powers and Functions of the Central Bank with respect to the National Payment System as set out in the Central Bank Law

In addition to the powers and function of each Central Bank with respect to the regulation and oversight of the National Payment System as set out in the primary National Payment System Act, all fourteen Central Banks also derive their mandate from provisions contained in the Central Bank Act. The benchmark in this regard is section 10(1)(c)(i) of the South African Reserve Bank Act, 1989 (As Amended)⁴²⁰ that provides that the South African Reserve Bank may “perform such functions, implement such rules and procedures and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems.” It is important to note that reference is made to payment, clearing and settlement systems, leaving the scope wide enough to include both systemically important and non-systemically important payment systems.

⁴¹⁹ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 156.

⁴²⁰ Act 90 of 1989 (As Amended).

When provision contained in other Central Bank Acts are compared against the provision in the South African Reserve Bank Act, 1989 (As Amended) it is clear that most provisions fall short in a number of respects.

Article 3(2) of Law nº 16/10 Law of the *Banco Nacional de Angola* specifically mandates the *Banco Nacional de Angola* to execute, monitor and control monetary, exchange and credit, to manage the payment system and manage the currency under the economic policy of the country. Article 28 of Law nº 16/10 mandates the *Banco Nacional de Angola* with the organisation and supervision of clearing and payment systems and permits the *Banco Nacional de Angola* to conclude, on their behalf or on behalf of the State and by the order of this, with similar public or private institutions domiciled abroad, clearing and payments agreements or any agreements that serve the same purpose.” These provisions only refer to the “management” of the National Payment System and do not specifically confer the powers of monitoring, oversight and supervision of payment, settlement and clearing systems.

The Bank of Botswana Act, 1996⁴²¹ contains one provision relevant to the role of the Bank of Botswana in the National Payment System. Section 4(1) states that, “the principal objectives of the Bank shall be first and foremost to promote and maintain monetary stability, an efficient payments mechanism and the liquidity, solvency and proper functioning of a soundly based monetary, credit and financial system in Botswana.” No explicit detail is provided on the regulatory, supervisory and oversight functions of the Central Bank. This provision only refers to the “promotion and maintenance of an efficient payments mechanism” and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

The DRC Act nº 005/2002 of 7 May 2002 on the Establishment, Organisation and Functions of the Central Bank of Congo is the Act that governs the Central Bank in the DRC. This Act only contains one provision covering the role, powers and functions of the Central Bank in the National Payment System. Article 6 of the Act requires the Central Bank to “execute all the duties of the Central Bank, namely: to promote the effective performance of the compensation and payment systems.” Article 6 only refers to the “promotion of the effective performance of payment systems” and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

In the absence of a legally enforceable National Payment System Act, the Central Bank of Lesotho derives its mandate to regulate and oversee the National Payment System from three provisions in the Central Bank of Lesotho Act, 2000.⁴²² Section 6(h) of the Central Bank of Lesotho Act, 2000 requires the Bank to promote the efficient operation of the payments system. Section 7(p) of the Central Bank of Lesotho Act, 2000 permits the Central Bank to promote the establishment of a financial institutions clearing system and provide facilities therefor and finally, section 50 permits the Central Bank to facilitate the clearing of cheques and other credit instruments for licensed institutions carrying on business in Lesotho. In addition, the Bank may, at any appropriate time and in conjunction with other licensed institutions, organise a clearing house and provide facilities therefor in Maseru and in such other place or places as may be desirable. Section 6(h) of the Central Bank of Lesotho Act, 2000 is of general application and only refers to the “promotion of efficient payment systems” and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

The Reserve Bank of Malawi also currently derives its mandate to regulate and oversee the National Payment System from sections 4(e) and section 45 of the Reserve Bank of Malawi Act (As Amended)⁴²³ as the Payment

⁴²¹ Act 19 of 1996.

⁴²² Act 2 of 2000.

⁴²³ [Chapter 44:02] (As Amended)

Systems Bill has not been passed. Section 4(e) of the Reserve Bank of Malawi Act (As Amended) states that, one of the principal objectives of the Bank is to promote a sound financial structure in Malawi, including payment systems, clearing systems and adequate financial services. In terms of Section 45 of the Reserve Bank of Malawi Act (As Amended), the Bank is permitted to promote money transfer and clearing systems and provide facilities therefor. This provision is also of general application and only refers to the “promotion of sound financial structure in Malawi, including payment systems, clearing systems and adequate financial services.”

In the absence of a legally enforceable National Payment System Act and with no National Payment System Bill on the table, the Bank of Mauritius derives its mandate to regulate and oversee the National Payment System solely from section 5(1)(c) of the Bank of Mauritius Act, 2004.⁴²⁴ Section 5(1)(c) reads, “The Bank shall have such functions as are necessary to achieve the attainment of its objects and, in particular, it shall manage, in collaboration with other relevant supervisory and regulatory bodies, the clearing, payment and settlement systems of Mauritius.” Section 5(1)(c) is of general application and only refers to the “management of clearing, payment and settlement systems in Mauritius.” The provision does not specifically refer to the monitoring, oversight and supervision of payment, settlement and clearing systems. Section 48(2) of the Bank of Mauritius Act, 2004 empowers the bank to set up such electronic system as it deems fit for the settlement of payments and participate in other ways in the settlement of payments. Section 48(6) also empowers the Bank to issue instructions or may make regulations under section 70 for the smooth functioning of a clearinghouse and payments system.

In addition to the powers and function of the *Banco de Moçambique* with respect to the regulation and oversight of the National Payment System as set out in Law n° 02/08 the BM also derives its mandate from Articles 31, 37, 38, 39 and 43 of Law n° 1/92 of 3 January Organic Law of the *Banco de Moçambique*. Article 31 of Law n° 1/92 permits the Bank, on its own behalf or on behalf and for the account of the State, to enter into clearing and payment agreements or any other contracts that serve the same purpose, with similar public or private institutions domiciled abroad.

Article 37 of Law n° 1/92 of 3 January Organic Law of the *Banco de Moçambique* is a general provision on the supervision of financial institutions.⁴²⁵

Article 38 of Law n° 1/92 of 3 January Organic Law of the *Banco de Moçambique* gives the *Banco de Moçambique* the power to conduct inspections.⁴²⁶ Article 39 of Law n° 1/92 of 3 January Organic Law of the *Banco de*

⁴²⁴ Act 34 of 2004.

⁴²⁵ Article 37(1) reads, “for the purposes of this diploma, all credit institutions and such other institutions as are determined by law shall be subject to supervision by the Central Bank, except for insurance companies.” Article 37(2) reads, “in order to ensure the supervision of the institutions subject to it, the Bank shall, in particular: a) consider and give its opinion on applications [for authorisation] to form and operate the said institutions, and on the merger, demerger or transformation of such institutions, and propose the revocation of authorisations that have been so granted, where necessary; b) define the conditions upon which subsidiaries, branches, agencies and other forms of representation of the said institutions may be opened up within the country and abroad, and decide on the applications submitted for this purpose; c) assess the suitability of the shareholders in these institutions, when such shareholders represent more than ten per cent of the share capital, as well as evaluate the technical and professional capacity of their general managers or directors and establish the mandatory requirements for the performance of these functions; d) issue directives on the operation of these institutions; e) ensure that there are services for the centralisation of credit risks and data.”

⁴²⁶ Article 38 reads, “(1)The Bank shall have power to carry out inspections of the establishments of financial institutions that are subject to its supervision in accordance with the law. (2) When performing their functions, the Bank staff responsible for carrying out the inspections shall have the proper credentials and they shall enjoy the attributes and powers of agents of the State.”

Moçambique requires that all institutions subject to supervision must send to the Bank, in accordance with the Bank's instructions, monthly balance sheets and other information relating to their situation and to the operations they perform. Article 43 that reads, "clearing of cheques and other credit instruments shall take place in the Bank, on terms to be established by special regulations."

Section 3(b) of the Bank of Namibia Act, 1997⁴²⁷ lists the "promotion and maintenance of internal and external monetary stability and an efficient payments mechanism" as one of the objectives of the Bank. This provision only refers to the "promotion and maintenance of an efficient payments mechanism" and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

The Central Bank of Seychelles also derives its mandate from section 30 of the Central Bank of Seychelles Act, 2004 (As Amended).⁴²⁸ Section 30 allows the Central Bank to establish or assist banks and other institutions in establishing facilities for the clearing and settlement of payments, including payments by cheques and other payment instruments, and may issue such directions relating thereto as it deems appropriate. Section 30, while giving the Bank power to issue directions with respect to the "establishment of facilities for the clearing and settlement of payments" does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

The Central Bank of Swaziland (Amendment) Act, 2004⁴²⁹ contains three provisions pertaining to the role of the Central Bank of Swaziland in the National Payment System. In terms of Section 4(f) of the Central Bank of Swaziland (Amendment) Act, 2004, one of the objects of the Bank is the promotion, regulation and supervision of efficient and secure operations of payment systems. Section 42(a) provides the Central Bank with the power to, at the appropriate time and in agreement with banks organise facilities for the clearing of cheques and other instruments for effecting payments. Section 42(b) specifically mandates the Bank, to; at the appropriate time and in agreement with banks supervise clearinghouses and other organised systems for the making of payments. Section 4(f) does not specifically confer the powers of monitoring and oversight of payment, settlement and clearing systems.

In the absence of a legally enforceable National Payment System Act, the Bank of Tanzania derives its mandate to regulate and oversee the National Payment System from five provisions in the Bank of Tanzania Act, 2006.⁴³⁰ Section 6(1)(a) of the Bank of Tanzania Act, 2006 mandates the Bank to "regulate, monitor, and supervise the payment, clearing and settlement system including all products and services thereof." Section 6(1)(b) specifically refers to the oversight function of the Bank of Tanzania and reads, "the Bank shall conduct oversight functions on the payment, clearing and settlement systems in any bank, financial institution or infrastructure service provider or company." In terms of section 6(2)(a) of the Bank of Tanzania Act, 2006, the Bank of Tanzania is permitted to participate in payment, clearing and settlement systems and as per section 6(2)(b), Bank of Tanzania may establish and operate any system for payment, clearing or settlement purposes. Section 6(2)(c) permits the Bank to perform the functions assigned by or under any other written law for the regulation of payment, clearing and settlement systems, providing scope for the function that will be legally mandated once the National Payment System Bill is passed into law.

⁴²⁷ Act 15 of 1997.

⁴²⁸ Act 12 of 2004 (As Amended).

⁴²⁹ Act 1 of 2004.

⁴³⁰ Act 4 of 2006.

In addition to the powers and function of the Bank of Zambia with respect to the regulation and oversight of the National Payment System as set out in the National Payment Systems Act, 2007⁴³¹, the Bank of Zambia also derives its mandate from provisions found in the Bank of Zambia Act, 1996.⁴³² The Bank of Zambia is specifically mandated in terms of section 4(2)(b) of the Bank of Zambia Act, 1996 to “promote efficient payment mechanisms.” Section 44 of the Bank of Zambia Act, 1996 provides further that the Bank of Zambia may, “in conjunction with other financial institutions, organise facilities for the clearing of their cheques and other instruments for effecting payments; and for this purpose organise a clearing system in Lusaka and elsewhere: Provided that only commercial banks at the discretion of the Bank may be permitted to maintain settlement accounts with the Bank.” Section 4(2)(b) only refers to the “promotion of efficient payment mechanisms” and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems.

The Reserve Bank of Zimbabwe derives its mandate from four provisions found in the Reserve Bank of Zimbabwe Act, 1999.⁴³³ Section 6(1)(e) of Reserve Bank of Zimbabwe Act, 1999 lists one of the functions of the Reserve Bank of Zimbabwe as the supervision of banking institutions and the promotion of the smooth operation of the payment system. In terms of section 12 of Reserve Bank of Zimbabwe Act, 1999, the Reserve Bank of Zimbabwe may, “assist banking institutions in organising facilities for the clearing and settlement of inter-bank payments, including payments by cheque or other instruments, and may for that purpose, establish such procedures and issue such directions to banking institutions as it considers appropriate.” Section 48 of the Reserve Bank of Zimbabwe Act, 1999 permits the Reserve Bank of Zimbabwe to either for its own account or for the account of or by order of the State, enter into clearing and payment agreements or any other similar agreement with public or private central clearing institutions outside Zimbabwe. Section 6(1)(e) of the Reserve Bank of Zimbabwe Act, 1999 only refers to the “promotion of the smooth operation of payment systems” and does not specifically confer the powers of monitoring, oversight, supervision and regulation of payment, settlement and clearing systems (although section 12 does permit the Reserve Bank of Zimbabwe to issue directions).

Section 10(1)(c)(i) of the South African Reserve Bank Act, 1989 (As Amended)⁴³⁴ is the most comprehensive provision contained in any Central Bank Act in the SADC region and should be seen as a best practice benchmark.

5.2.1.2 Powers and Functions of the Central Bank with respect to the National Payment System as set out in the National Payment System Act

Table 36 below provides a consolidated view of all of the provisions pertaining to the powers and functions of Central Banks with respect to the National Payment System as found in the National Payment System Act / Clearance and Settlement System Act / Payment System Management Act in each country.

It is important to acknowledge that different countries apply different approaches (this is particularly so with respect to the authorisation, licensing, designation, or recognition of payment systems, payment system operators, participants and instruments), but at the same time, there is a need to standardise and harmonise the approach taken in the SADC region. An example of a harmonised approach is found in Articles 6 and 10 of

⁴³¹ Act 1 of 2007.

⁴³² [Vol 20 Chapter 360].

⁴³³ [Chapter 22:15].

⁴³⁴ Act 90 of 1989 (As Amended).

the Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC) that requires Member States to notify to the Commission of which systems and respective system operators they have designated and which national authorities are in charge of notification. The Commission holds two registers with this information. They are up-dated whenever Member States send new information to the Commission. Article 10(1) of the Settlement Finality Directive 98/26/EC (As Amended) reads: "Member States shall specify the systems, and the respective system operators, which are to be included in the scope of this Directive and shall notify them to the Commission and inform the Commission of the authorities they have chosen in accordance with Article 6(2). The system operator shall indicate to the Member State whose law is applicable the participants in the system, including any possible indirect participants, as well as any change in them. In addition to the indication provided for in the second subparagraph, Member States may impose supervision or authorisation requirements on systems which fall under their jurisdiction. An institution shall, on request, inform anyone with a legitimate interest of the systems in which it participates and provide information about the main rules governing the functioning of those systems."⁴³⁵

Where a country has elected not to empower the Central Bank, together with licensed banking institutions to form a juristic person (Payment System Management Body) and to confer certain powers and functions on the juristic body, it should follow that these powers and functions should remain with the Central Bank and be reflected in the National Payment System Act accordingly. It is however evident from the analysis presented in the table below that several Acts have substantial gaps and many of the powers and functions that should be conferred on the Central Bank by the National Payment System Act, are not.

Areas of particular concern include: the lack of specific oversight provisions in several Acts; the specific mandate for the Central bank to operate a settlement system and participate in such a system; very few provisions on allowable sponsorship arrangements; few provisions on payment service providers and even fewer provisions on payment instruments. Several Acts contain no provisions on inspections and investigations. Perhaps the most glaring gap in several Acts is the lack of provisions pertaining to the power to issue Regulations, Directives and Guidelines and to impose administrative sanctions. It is also important to note that only three SADC Member States have provisions in their Acts requiring the Central Bank to cooperate with other domestic regulatory authorities and international regulatory authorities.

⁴³⁵ Article 10(2) states that, "a system designated prior to the entry into force of national provisions implementing Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial collateral arrangements as regards linked systems and credit claims shall continue to be designated for the purposes of this Directive. A transfer order which enters a system before the entry into force of national provisions implementing Directive 2009/44/EC, but is settled thereafter shall be deemed to be a transfer order for the purposes of this Directive."

Table 36: Gap Analysis and Comparative Review: Powers and Functions of the Central Bank as set out in the National Payment System Act / Bill

POWERS AND FUNCTIONS	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
EXERCISE POWERS AND FUNCTIONS CONFERRED BY THE ACT															
Central Bank required to exercise the powers and perform the functions conferred by the Act	✓	✓	✗	●	●	*	✓	✓	✗	✓	✓	*	✓	✓	10
Central Bank required to ensure the safe, secure, efficient and cost effective operation of the National Payment System	✗	✗	✗	●	●	*	✓	✓	✗	✓	✗	✗	✓	✗	6
PUBLIC INTEREST OBJECTIVES															
Ensure that the standards, criteria and conditions determined by it have the effect of encouraging appropriate payment system co-operation	✗	✗	✗	PAL	✗	✗	✗	PAN	✗	PASA	✗	✗	✗	✗	3
Ensure that the standards, criteria and conditions determined by it have the effect of ensuring fair access by system participants to payment	✗	✗	✗	PAL	✗	✗	✓	PAN	✗	✗	✗	✗	✗	✗	3
Ensuring compliance with the public interest objectives as set out in the Law	✓	✗	✗	✗	✗	✗	✓	✓ ⁴³⁶	✗	✗	✗	✗	✗	✗	3
Formulate and approve of standards enabling full accomplishment of public interest objectives	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
Withdraw/revoke recognition/authorisation/designation of a recognised / authorised/designated system if it is in the public interest	✗	✓	✗	✗	●	✗	✗	✗	✓	✓	✓	✗	✗	✓	6
Dissolve subsystems and chambers, as long as this is intended for the fulfilment of public interest objectives	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	1
MANAGEMENT & COORDINATION															
Manage the payment system	✗	✗	●	PAL	✗	*	✓	PAN	✗	PASA	✗	✗	✗	✗	5
Central Bank must coordinate the payment system	✗	✗	✗	✗	✗	✗	✓	PAN	✗	✗ ⁴³⁷	✗	✗	✗	✗	2

⁴³⁶ The Payment System Management Amendment Act 18 of 2003 gives the bank the powers to set standards for fees and charges in the interest of the public. Section 13 of the payment System Management Act, 2003 allows directives to be issued if there is behavior not in public interest.

⁴³⁷ Although not expressly stated in the National Payment System Act 79 of 1998 (As Amended), the management and coordination of the National Payment System is implied (sections 3 and 4).

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
OVERSIGHT															
Specific provision on Central Bank oversight	✓	×	×	●	●	×	✓	✓	×	×	×	*	✓	×	6
Oversee the issuance and use of the payment instruments	×	×	×	●	×	×	✓ ⁴³⁸	✓	×	×	×	×	×	×	3
Ensure that the standards, criteria and conditions determined by the PSMB have the effect of facilitating oversight of the National Payment System by the Bank	×	×	×	PAL	×	×	×	PAN	×	×	×	×	×	×	2
MONITORING															
Central Bank must monitor the National Payment System, system participants and service providers	×	×	●	×	×	×	✓	✓	×	×	×	×	×	×	3
Monitor and regulate clearance and settlement systems and the activities of participants	×	✓	●	×	×	×	✓	PAN	×	×	✓	×	✓	×	6
ESTABLISH AND OPERATE A SETTLEMENT SYSTEM															
Central Bank may establish and operate a settlement system	×	✓	×	●	×	*	✓	✓	✓	×	✓	*	×	✓	7
Participate in the settlement system	×	×	×	×	×	×	×	✓	×	×	×	×	✓	×	2
Enter into settlement contracts between the Bank and system participants	×	×	×	×	●	×	×	✓	×	×	×	×	×	×	2
Determine conditions, rules or procedures regarding the issuing of settlement instructions and discharging of settlement obligations	×	✓	●	×	●	×	✓	✓	✓	×	✓	×	×	✓	8
Provide an external audit of systems operated by the Central Bank	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	1
ESTABLISH A JURISTIC PERSON: PSMB															
Together with banking institutions, cause to be established by a constitution a juristic person known as the Payment System Management Body	×	×	×	PAL	×	×	×	✓	×	×	×	×	×	×	2
Be a member of the PSMB	×	×	×	●	×	×	×	✓	×	✓	×	×	×	×	3
Approve any amendment to the constitution or rules of the PSMB	×	×	×	●	×	×	×	✓	×	✓	×	×	×	×	3

⁴³⁸ See Aviso n° 1/GBM/2014 on the Regulation of Bank Cards.

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
Approve the dissolution of the PSMB	x	x	x	●	x	x	x	✓	x	✓	x	x	x	x	3
CONSTITUTION OR RULES OF A SYSTEM															
Approval of amendments to the constitution of a recognised system, or to the rules governing the system	x	✓	x	x	x	x	x	✓	✓	x ⁴³⁹	✓	x	x	✓	5
Keep a copy of the constitution / rules of the system at the offices of the Central Bank	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	✓	4
AUTHORISATION															
Authorisation of persons to participate in the clearing systems	x	x	x	●	x	x	x	✓	x	x	x	x	x	x	2
Authorisation of persons to participate in the settlement system	x	x	x	●	x	x	x	✓	x	x	x	x	x	x	2
Authorisation of the operation of the PSMB (juristic person)	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Authorise a person to provide any payment system service without being registered with the body as a service provider	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Withdrawal of authorisation of persons to participate in the clearing systems	x	x	x	●	x	x	x	✓	x	x	x	x	x	x	2
Withdrawal of authorisation of persons to participate in the settlement system	x	x	x	●	x	x	x	✓	x	x	x	x	x	x	2
Authorise payment, clearing and settlement systems operators	x	x	x	x	●	x	x	PAN	x	x	x	x	x	x	2
Prohibit, by written order, the operation of a payment, clearing and settlement system	x	x	x	x	●	x	x	✓	x	x	x	x	x	x	2
Authorise the establishment / functioning of subsystems and chambers	✓	x	x	x	x	x	✓	x	x	x	x	x	x	x	2
Regulate subsystems and chambers	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	1
Regulate access criteria to the subsystems and chambers	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	1
Regulate procedures and criteria for the withdrawal of any participant	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	1

⁴³⁹ This is however implied in both the South African Reserve Bank and National Payment System Acts and current practices at PASA level..

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
LICENSING OF PAYMENT SYSTEM OPERATORS															
License a system operator	x	x	x	●	●	x	x	x	x	x	x	x	x	x	2
Grant or refuse the application for a license to operate a system	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
Withdraw or suspend a license to operate a system	x	x	x	●	●	x	x	x	x	x	x	x	x	x	2
Recommend criteria for persons to be authorised to act as payment system operators / PCH operator	x	x	x	PAL	x	x	x	x	x	PASA	x	x	x	x	2
Authorise person to act as a payment system operator / PCH operator	x	x	x	PAL	x	x	x	x	x	PASA	x	x	x	x	2
DESIGNATION															
Designate a particular payment system	x	x	x	x	x	x	x	x	x	✓	x	x	✓	x	2
Designate a settlement system	x	x	x	x	x	x	x	x	x	✓	x	x	✓	x	2
Place a notice in the Government Gazette, to give notice to the operator of the system of the designation	x	x	x	x	x	x	x	x	x	✓	x	x	✓	x	2
Vary or revoke any designation	x	x	x	x	x	x	x	x	x	✓	x	x	✓	x	2
Designate a clearing system participant by notice in the Gazette	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	1
Vary or revoke any designation of a clearing system participant	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	1
Prescribe the requirements to be complied with by an applicant who intends to operate a payment system that is to be designated	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Determine an application for designation within a period of 90 days	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Register the applicant for designation and grant a certificate of designation	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Refuse to register an applicant or grant a certificate of designation of a payment system where the applicant does not comply with the requirements for designation	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Designation of payment system businesses	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Grant a certificate of designation to the payment system business	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
Designate by way of regulations, widely accepted international standards and practices	x	x	x	●	x	x	x	x	x	x	x	x	x	x	1
RECOGNITION															
Recognise a clearance and settlement system	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	✓	4
Recognise different clearance and settlement systems in respect of different classes of financial institutions, different areas, for the clearance of different classes of obligations	x	✓	x	x	x	x	x	x	x	x	✓	x	x	✓	3
Recognise a PSMB (juristic person)	x	x	x	●	x	x	x	x	x	✓	x	x	x	x	2
Withdraw recognition of PSMB (juristic person)	x	x	x	●	x	x	x	x	x	✓	x	x	x	x	2
Before withdrawing recognition of a recognised system, notify the system's management body, in writing, that it is considering doing so and of its reasons for considering such a step and give the management body an opportunity to make representations on the matter	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	✓	4
Withdrawal of recognition of a management body	x	✓	x	x	x	x	x	x	✓	x	✓	x	x	✓	4
SPONSORSHIP															
Recommend criteria for sponsorship arrangements	x	x	x	PAL	x	x	x	✓	x	PASA	x	x	x	x	3
PAYMENT SERVICE PROVIDERS															
Register a person who is not a payment system participant as a service provider	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Authorise PSP to provide one or more payment system services	x	x	x	PAL	●	x	x	PAN	x	x	x	x	x	x	3
Cancel the registration of a service provider if the service provider contravenes or fails to comply with any terms or conditions of its registration	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Central bank may decide that any service provider discontinue to provide payment services	✓	x	x	x	x	x	x	✓	x	x	x	x	x	x	2
PAYMENT SYSTEM BUSINESSES															
Oversee the operation of payment system businesses	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
Prescribe the requirements to be complied with for designation as a payment system business	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
PAYMENT INSTRUMENTS															
Determine and administer payment instrument standards / norms	x	x	●	●	x	*	✓ ⁴⁴⁰	PAN	x	x	x	x	x	x	4
Receive and review applications for the registration of payment instruments	x	x	●	x	x	x	x	✓ ⁴⁴¹	x	x	x	x	x	x	2
Regulate payment instruments	✓	x	x	x	x	x	✓ ⁴⁴²	✓	x	x	x	x	x	x	3
License or authorise the issuance of payment instruments	x	x	●	x	●	x	x	✓ ⁴⁴³	x	x	x	x	x	x	3
Prohibit, by written order, any person from issuing or using a payment instrument	x	x	●	x	●	x	x	x	x	x	x	x	x	x	2
Monitor and govern payment instruments	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
Determine the rules / provisions for the reimbursement of funds from un-authorized or defective transactions	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
Set the acceptable time period between the delivery of the instrument or initial payment and the moment when the beneficiary account is credited	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
ELECTRONIC MONEY															
Determine the terms and conditions for approval of any person wishing to be an institution issuing and distributing E-Money as its main or secondary occupation	x	x	●	x	x	x	x	✓	x	x	x	x	x	x	2
Determine the prudential regulation specific to issuance and/or distribution of E-Money	x	x	●	x	x	x	x	✓	x	x	x	x	x	x	2
INSPECTIONS AND INVESTIGATIONS															
Central Bank may undertake inspections	✓	x	●	●	●	x	✓	✓	x	x	x	x	✓	x	7
Central Bank may conduct investigations	x	x	x	●	●	x	x	✓	x	x	x	x	✓	x	4
Give instructions to external auditors	✓	x	●	x	x	x	✓	x	x	x	x	x	x	x	3

⁴⁴⁰ See the general provision – Article 17(4) Law n° 02/08 of 27 February.

⁴⁴¹ Namibia is only one of two countries that require persons wishing to issue a payment instrument to register the instrument with the Bank. Only a person that is a system participant or a person exempted by the Minister under subsection (2) or a category of exempted persons may register and issue a payment instrument (section 5(1)).

⁴⁴² See the general provision – Article 17(4) Law n° 02/08 of 27 February.

⁴⁴³ See PSD-1 Determination on Issuing of a Payment Instrument

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
REPORTS, RETURNS AND INFORMATION															
Have access to information and documentation	✓	✓	●	●	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	12
Reports, returns and other information on: the volumes and values of transfer instructions cleared in the system; volumes and values of the participants' payment obligations and settlement obligations, any other information regarding the operation of the system	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓	6
Obtain reports from any person or institution involved in payment intermediation and require such institutions to adopt or conform to specified operating requirements	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	3
Request information on: liquidity and solvency levels	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1
Request information on: the risks that operators, PSPs and participants face	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1
Request information on: the security, control and backup procedures used by operators, PSPs and participants on their communication and computer systems	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1
Request information on: compliance with norms, laws and regulations governing operations	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1
Request information on: charges and commissions	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	1
GUIDELINES															
Issue guidelines	✗	✗	✗	✗	●	✗	✗	✗	✗	✗	✗	✗	✓	✗	2
DIRECTIVES															
Issue directives to any person participating in the National Payment System	✗	✓	●	●	●	✗	✗	✓	✓	✓	✓	✗	✓	✓	10
Apply to the High Court for an order directing such person to comply with a directive	✗	✓	✗	✗	●	✗	✗	✓	✓	✓	✓	✗	✗	✓	8
Issue directives implementing the provisions of the Act	✗	✗	✗	✗	●	*	✗	✓	✗	✓	✗	✗	✗	✗	3
ADMINISTRATIVE PENALTIES															
Central Bank may impose administrative penalties	✗	✗	●	●	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	3

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
TECHNICAL POLICIES, CRITERIA, STANDARDS, MESSAGE FORMATS															
Determine and administer operational and technical policies	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Determine and administer operational and technical criteria, conditions and standards	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Determine and administer electronic notification and messaging standards	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Determine and administer formats for electronic files	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
Define the Terms and Conditions for the functioning of payment subsystems	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
Set the Terms and Conditions for Interoperability	x	x	●	x	x	x	x	x	x	x	x	x	x	x	1
RULES AND REGULATIONS															
Central Bank may issue Determinations (by notice in the Gazette)	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	1
Central Bank may prescribe rules and arrangements relating to the operation of payment systems	x	x	x	x	x	x	✓	x	x	x	x	x	✓	x	2
Central Bank may make regulations / regulatory guidelines	✓	x	x	●	x	*	✓	x	✓	x	x	x	✓	x	5
Minister may make regulations	x	✓	x	x	●	x	x	x	x	x	✓	*	✓	x	
EXEMPTIONS															
Exempt any class of participants from provisions of Act	x	x	x	x	x	x	x	✓	x	x	x	x	✓	x	2
Provide for a variation or revocation of an exemption by notice published in the Government Gazette	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	1
RECORDS															
Central Bank to retain records (Number of Years Indicated)	5	x	x	x	7	x	x	5	7	5	x	x	x	x	5
Manner in which records to be kept is specified	✓	x	x	x	●	x	x	x	✓	✓	x	x	x	x	4
CERTIFICATION															

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
Certify that payment systems, clearing systems & payment system services meet standards, criteria & conditions	x	x	x	PAL	x	x	x	PAN	x	x	x	x	x	x	2
FORUM															
PSMB may act as a forum for the consideration of matters of policy and mutual interest	x	x	x	PAL	x	x	x	PAN	x	PASA	x	x	x	x	3
System Management Body may provide a forum for the consideration of matters of mutual interest	x	✓	x	x	x	x	x	✓	x	PASA	✓	x	x	✓	5
System Management Body may act as a medium of communication on behalf of its participants with the Government, Central Bank and other regulatory authorities	x	✓	x	x	x	x	x	x	x	PASA	✓	x	x	✓	4
ACT AS AN ARBITRATOR															
Act as arbitrator in conflicts between participants in the payment system	x	x	x	x	x	x	✓	x	x	x ⁴⁴⁴	x	x	x	x	1
INSTITUTE PROCEEDINGS															
Central Bank is responsible for instituting proceedings and making decisions on the contravention of the Law	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	1
COOPERATION WITH OTHER REGULATORY AUTHORITIES															
Cooperation with other domestic regulatory authorities	✓	x	x	x	✓	x	✓	x	x	x	x	x	x	x	3
Cooperation with other international regulatory authorities	✓	x	x	x	✓	x	✓	x	x	x	x	x	x	x	3

⁴⁴⁴ In practice, disputes are referred to the South African Reserve Bank as an industry norm if PASA is unable to resolve them.

5.3 Confidentiality, Disclosure of Information and Indemnity

The National Payment System Act should contain provisions on the confidentiality of information, prohibition against the use of information for personal gain, conditions for the disclosure of information and indemnity of the Central Bank and other officials. As indicated in Table 37 below, the Draft National Payment System Law in the DRC and the Malawian and Lesotho Bills do not contain several of the provisions found in the Acts applicable in other SADC Member States. In the absence of a National Payment System Act, none of these provisions, as they relate to the National Payment System are found in Mauritian law or regulation.

Only two National Payment System Acts and one National Payment System Bill contain an indemnity provision for officers or persons employed by the Central Bank or by any other person in the exercise or performance or purported exercise or performance, in good faith, of any power or function under the Act. The Namibian Payment System Management Act, 2003⁴⁴⁵ contains all of the provisions bar the provision that the confidentiality of information provisions does not apply to the disclosure of information that is generally known to members of the public or a substantial section of the public.

Table 37: Gap Analysis and Comparative Review: Confidentiality, Disclosure and Indemnity

CONFIDENTIALITY, DISCLOSURE & INDEMNITY															
CONFIDENTIALITY OF INFORMATION															
Information obtained by the Central Bank may not be disclosed by any director or officer of the Central Bank to any person	✓	✓	✗	✗	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	10
PROHIBITION AGAINST USE OF INFORMATION FOR PERSONAL GAIN															
Any officer or employee of the Central Bank that uses information acquired during the performance of his functions under the Act shall be guilty of an offence	✓	✓	✗	✗	✗	✗	✗ ⁴⁴⁶	✓	✓	✓	✓	✗	✗	✓	7
CONDITIONS FOR THE DISCLOSURE OF INFORMATION															
Central Bank may disclose any information whose disclosure is, in its opinion necessary and in the public interest to protect the integrity, effectiveness or security of the National Payment System	✓	✓	✗	✗	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	10

⁴⁴⁵ Act 18 of 2003 (As Amended).

⁴⁴⁶ This provision is not contained in Law n° 02/08 of 27 February. However, anyone who has access to information because of the exercise of the activity in the *Banco de Moçambique* (Employees and any person) is subject to professional secrecy, in accordance with Article 74 of the Organic Law of the *Banco de Moçambique* (is forbidden to disclose or use for any purpose). Any violation committed is an offence punishable under Article 290 of the Criminal Code (Violation of Professional Secrecy).

The confidentiality of information provisions does not apply to any disclosure made by a person in the performance of his functions under the Act or under the constitution or rules of any recognised payment system	x	✓	x	x	x	x	x ⁴⁴⁷	✓	✓	✓	✓	x	✓	✓	7
The confidentiality of information provisions does not apply when required by a court of law	x	✓	x	x	x	x	x	✓	✓	✓	✓	x	✓	✓	7
The confidentiality of information provisions does not apply to the disclosure of information that is generally known to members of the public or a substantial section of the public	x	✓	x	x	x	x	x	x	✓	✓	✓	x	x	✓	5
INDEMNITY OF CENTRAL BANK AND OTHER OFFICIALS															
No act, matter or thing done by any officer or person employed by the Central Bank or by any other person in the exercise or performance or purported exercise or performance, in good faith, of any power or function under this Act shall give rise to any action, claim, liability, suit or demand against the officer or person concerned.	x	x	x	x	●	x	x	✓	*	x	x	x	✓	x	3

5.4 The Public Interest Objective

Most National Payment System Acts in force in SADC Member States make reference to the “public interest” several times without defining what the “public interest” is. For example, Section 15(2)(b) of Lesotho’s Payment Systems Bill, 2013 requires the Governor to, in considering whether or not to issue a directive in terms of section 15(1) to have regard to whether reasonable grounds exist to believe that any person is engaging in or is about to engage in any act, omission or course of conduct, with respect to the payment system that is likely to be contrary to the public interest.

Section 53 of the Namibian Payment System Management, 2003 (As Amended)⁴⁴⁸ reads, “The Minister, after consultation with the Bank, by notice in the Gazette and subject to such conditions as the Minister may determine, may exempt any person or category of persons from the provisions of subsection 5(1), if the Minister is satisfied that such exemption is in the *public interest* and will not cause undue risk to the National Payment System.” Other references to the public interest are found in sections 7(3)⁴⁴⁹ and 13(1) of the Namibian Payment System Management, 2003 (As Amended).⁴⁵⁰ Recognition of the public interest objective is

⁴⁴⁷ This provision is not found in Law n 02/08 of 27 February . However, see Article 74 of the Organic Law of the BM.

⁴⁴⁸ Act 18 of 2003 (As Amended).

⁴⁴⁹ Section 7(3) of the Payment System Management, 2003 (As Amended) reads, “The Minister, by notice in the Gazette, after consultation with the Bank and the Body, and subject to such conditions as the Minister may determine, may exempt any person or category of persons from section 7 (1), if the Minister is satisfied that such exemption is in the public interest and will not cause undue risk to the national payment system.” Section 7(1) covers the prohibition against payment intermediation.

⁴⁵⁰ Section 13(1) of the Payment System Management, 2003 (As Amended) reads, “if the Bank knows or reasonably believes that any person participating in the national payment system engages in or is about to engage in any act, omission or course of conduct, that results or is likely to result in systemic risk, or is detrimental to or may be detrimental

also seen in section 3(5) of the Payment System Management, 2003 (As Amended) that requires the PSMB to ensure that the standards, criteria and conditions determined by it under section 3(4)(a) have the effect of (a) encouraging appropriate payment system co-operation and competition in the provision of payment system services; (b) ensuring fair access by system participants to payment system services.

Article 6(1) of Zimbabwe’s National Payment Systems Act [Chapter 24:23] empowers the Reserve Bank of Zimbabwe, by notice in writing to the management body of the system concerned, withdraw its recognition of a recognised system if the Bank has reasonable grounds for believing that (a) the system no longer fairly represents the interests of all financial institutions that are or should become participants in the system; (b) the management body has contravened any provision of this Act or of the system's constitution; or (c) the manner in which the system is being conducted does not adequately protect the system against systemic risk, and that it is in the public interest to withdraw its recognition from the system concerned.” Further, the Minister after consultation with the Reserve Bank may, by notice in the Gazette exempt any persons or class of persons from the provisions of subsection 17(1) if the Minister is satisfied that such an exemption will be in the public interest and will not cause undue risk to any recognised payment system (section 17(4)).⁴⁵¹

In contrast to the general public interest statements found in most National Payment System Acts in force in SADC Member States, two countries in the SADC region, namely Angola and Mozambique include specific public interest objectives in their National Payment System Act. Table 38 below sets out the provisions found in the Mozambican Law n° 2/2008 Law on the National Payment System. Should all fourteen SADC countries elect to draft a Model Payment System Act, it is strongly recommended that the “public interest” is defined and that a provision such as the Mozambican provision be included in the model law. In addition to the five articles found in the Mozambican law, a provisions covering *inter alia*: co-operation and competition and consumer protection should be considered.

Table 38: Public Interest Objective Provisions found in Law n° 2/2008

Example: Law n° 2/2008 Law on the National Payment System (Mozambique)		
Article 4(1)	Public interest objectives	Payment systems must fulfil public interest objectives, namely: a) security; b) reliability; c) transparency; d) efficiency.
Article 4(2)	Security Objective: Payment systems to be provided with appropriate infrastructure, operated by qualified staff and have transparent rules	To comply with the security objective, payment subsystems shall be provided with appropriate infrastructures consistent with internationally acceptable standards for similar operations and be operated by duly qualified staff in accordance with appropriate and transparent rules for purposes of: a) controlling credit, liquidity, legal, operational and systemic risks; b) containing risks to the Central Bank arising from its responsibilities as financial settlements agent; c) immediate, automatic and unconditional execution of guarantees provided.

to, or is or will be contrary to the public interest in, the integrity, effectiveness or security of the national payment system, the Bank may issue a directive in writing.”

⁴⁵¹ Section 17(1) of Zimbabwe’s National Payment Systems Act [Chapter 24:23] is a prohibition against settlement intermediation.

Article 4(3)	Reliability Objective: Subsystems must have minimum operational continuity plans	In order to comply with the reliability objective, subsystems shall be endowed with minimum operational continuity plans to ensure that operations continue to be processed without interruption within the established timeframes, and shall possess backup systems to recover data in the case of failures or incidents.
Article 4(4)	Transparency Objective: Rules to be communicated to all participants	Compliance with the transparency objective requires that the subsystems possess their own set of rules to be communicated to all participants in a timely manner; final beneficiaries must be informed in advance of charges and timeframes for funds to be made available, and conditions for termination of payment services.
Article 4(5)	Efficiency Objective: Charges must be competitive and fair	To comply with the efficiency objective, subsystem operators must ensure that charges for services rendered are competitive and fair.

5.5 Access to Clearing and Settlement Systems

One of the key findings set out in the South African Banking Enquiry Report to the South African Competition Commission was that, "The existing regulatory regime for the National Payment System does not appear to meet the needs of South African consumers for competitive and technically innovative payment services. The approach of largely ignoring non-bank activities has begun to shift. But persistence in the view that only clearing banks may participate in clearing and settlement is not an approach that will best serve South Africa's interest. We are convinced of the need for a revision of the regulatory approach and the development of an appropriate regulatory regime for payment system activity which is functionality-based, rather than institutionally based, so as to ensure quality of access regardless of whether they are clearing banks or not."⁴⁵²

In most SADC Member States, access to clearing and settlement systems remains the exclusive domain of the Central Bank and Banks. Several Central Banks while mandated by the National Payment System Act to set access and participation criteria have not done so. In several cases, the domestic law is unclear on who has access to and may participate in the settlement system or clearinghouse. In other cases such as in Botswana, the provisions of the Law seem to be at odds with the stance taken by the Bank of Botswana that "membership of BISS is open to all clearing banks operating in Botswana as well as the Bank of Botswana" as section 3(3)(a)

⁴⁵² The three recommendations made by the Enquiry Panel with respect to access to the National Payment System were as follows: Recommendation 1: "An access regime that includes non-bank providers of payment services should be developed so as to allow for their participation, under effective regulation and supervision, in both clearing and settlement activities in appropriate low-value or retail payment streams. There are international precedents – such as those from Australia and the European Union – that suggest that an access regime of this sort can be designed that does not threaten the stability of the existing system. Recommendation 2: "**The National Payment System Act should be revised.** This would allow non-banks to be clearing and (even) settlement participants, and hence members of PASA. It would allow for different types of participants and membership of PCHs. Once the National Payment System Act has been redrafted, the associated South African Reserve Bank and PASA position papers and directives should have to be revised. Obvious examples are the Bank Models position paper, to accommodate the realities of Postbank and Ithala and the E-Money position paper, as well as the directives on system operators and third party providers." Recommendation 3: "The membership and governance of PASA should be revised so as to include qualified non-bank participants. In our opinion this position, together with the professed view of the NPSD that their remit and that of the payment system management body extends throughout payment system activity, means that PASA membership should be extended to participating non-banks."

of Botswana's National Clearance and Settlement Systems Act, 2003⁴⁵³ refers to "financial institutions" in the broader sense and not simply to licensed banks. Several Acts are silent on permissible sponsorship arrangements. In the absence of a legally enforceable National Payment System Act, the DRC, Lesotho, Malawi and Mauritius rely on various agreements, rules and Terms and Conditions to regulate access and participation, a situation that is far from ideal. In the section that follows, the substantive provisions as set out in each National Payment System Act or Bill are provided. The current stance taken by South Africa and Namibia are also discussed as an example of how the thinking of a number of Central Banks with respect to allowing non-bank participation in the clearing and settlement domain is changing. To date, Namibia is the only SADC Member State that has issued a legally binding Determination that sets out the criteria for authorisation and participation in clearing and settlement systems for both banks and non-bank participants. In line with Objective 2 of Namibia's *National Payment System Vision 2015*, namely that "the objective of this strategic focus area is to enable access to payment system, thereby promoting financial inclusion", section 8 of PSD-6 sets out the Bank of Namibia's position on designating non-bank financial institutions (NBFIs) for the purposes of participating in clearing and settlement systems.

In Angola, in terms of Article 7(4) of Law n° 5/05 Payment System of Angola the Central Bank is mandated to "authorise the functioning of subsystems and chambers, including those performing operations involving securities, such authorisation being subject to technical and technological ability of such subsystem and chamber to fulfil public interest objectives as well as to fulfill the provisions of the law." As per Article 7(2)(d) of Law n° 5/05 Payment System of Angola, the Central Bank is required to "formulate and approve standards enabling the full accomplishment of the public interest objectives and regulate issues relating to access criteria to the subsystem and chambers (clearing house) according to competitiveness in payment services." The Central Bank is also required in terms of Article 7(e) of Law n° 5/05 Payment System of Angola to formulate procedures and criteria for the withdrawal of any participant at their own request or at the proposal of a subsystem or chamber (clearing house) operator or by a decision by the Central Bank. While these provisions are of broad application, the law is unclear on who has access to and may participate in the settlement system or clearinghouse. The law contains no provisions on the authorisation of clearing system participants or on permissible sponsorship arrangements.

In Botswana, access and participation in the Botswana Interbank Settlement System (BISS) is regulated by the National Clearance and Settlement Systems Act, 2003. In terms of section 3(3)(a) of the National Clearance and Settlement Systems Act, 2003, the Central Bank will not recognise a clearance and settlement system unless it is satisfied that only financial institutions and the Central Bank are permitted to become participants in the system. A financial institution is defined in section 2 as (a) a person licensed under section 3 of the Banking Act to transact banking business in Botswana, or (b) a broker-dealer, insurance company, investment scheme, central securities depository or pension fund. As the definition of financial institution contained in the Botswanan National Clearance and Settlement Systems Act 2003 is broader than banks, it would appear that the Bank of Botswana's stance that "membership of BISS is open to all clearing banks operating in Botswana as well as the Bank of Botswana" is at odds with the provisions in the National Clearance and Settlement Systems 2003 as section 3(3)(a) refers to "financial institutions" in the broader sense and not simply to licensed banks. As per section 3(3)(d)(i) of the National Clearance and Settlement Systems Act 2003, the Bank of Botswana will not recognise a clearance and settlement system unless it is satisfied that the constitution and rules governing the system are fair, equitable and transparent and make adequate provision for admitting financial institutions into the system as participants and regulating and terminating their participation. The constitution and rules governing the system must also establish criteria according to which a participant may be authorised to introduce any person to provide payment services (section 3(3)(d)(v)).

⁴⁵³ Act 5 of 2003.

In terms of Articles 4 and 5 of the DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 the Central Bank is required to determine the rules for the functioning of the payment system carried out by the Central Bank and approve rules of payment systems carried on by a Third Party (Article 4). These rules, as specified in Article 5, must specify inter alia: the nature, the volume of activities and the number of the participants considered; define the admission, suspension and potentially exclusion conditions of the participants in the system; and define the rights and obligations of the participants arising from their participation in the system. The DRC has not issued clear criteria for authorisation of participants in the clearing and settlement systems.

In Lesotho, in the absence of a legally enforceable National Payment System Act, access to and participation in the RTGS system is currently governed by the Adhesion Agreement for the Participation to the Lesotho Wire System. In terms of Article 3(1) of the agreement, the following entities are entitled to participate in the system: Financial Institutions established in Lesotho as well as similar foreign banks duly supervised by another country; The Bank; The Lesotho Government as an indirect participant including the local agencies or authorities; Foreign Central Banks; Operators of domestic and foreign payment systems, clearing houses and securities settlement systems. In order to effectively become a participant, entities must comply with several technical requirements as set out in Annex A of the Adhesion Agreement. In terms of the Payment Association of Lesotho Electronic Funds Transfer Credit and Debit Clearing Rules, members must be clearing banks and accepted members under the Lesotho Wire Rules and the Payments Association of Lesotho. Each participant is required to conform to the entry and participation criteria laid down for membership of the PAL as articulated in the ACH rules and must have a signed PCH Agreement, the LSW Participant Agreement and any other appropriate agreement specified by the PCH PG. In terms of section 4.1.1.4, prior to commencing clearing activities in a payment stream, a prospective participant must be in possession of a written certification from an authorised PSO that it has met all the relevant technical operating standards and has successfully tested its operational capabilities in respect of payment instructions in the PCH. A participant that is sponsoring clearing services is required as per section 4.1.1.7 to assume all the obligations in the clearing process on behalf of the sponsored clearer under the agreement, which has been approved by the PAL with the sponsored clearer.⁴⁵⁴

Access criteria for the current Malawi Interbank Transfers and Settlement System (MITASS) system are set out in the Reserve Bank of Malawi's 2008 document entitled, *Access Criteria for RTGS System Participants*.⁴⁵⁵ In terms of section 3 of this document, the qualifying criteria for banks are: 1) they must have a commercial bank licence; 2) they must have access to Reserve Bank of Malawi lending; 3) they must be subject to the Liquidity

⁴⁵⁴ Section 8(3)(d) of the Payment System Bill, 2014 empowers the PSMB to recommend for approval by the Governor criteria subject to, and in accordance with which a member that is also a central bank settlement system participant may be authorised to (i) allow a bank, or branch of a foreign financial institution that is not a central bank settlement system participant to clear, or (ii) clear on behalf of a bank, or a branch of a foreign financial institution that is not a central bank settlement system participant, provided that the member settles payment obligations on behalf of such bank, or branch of a foreign banking institution. This is the same sponsorship arrangement set out in the South African National Payment System Act 78 of 1998 (As Amended). Section 4(2)(b) of the *Payment System Bill, 2013* lists the establishment and operation of a settlement system, the operations of the payment system and the authorisation of persons and service providers to participate in the clearing and settlement system activities and to withdraw such authorisation as one of the functions of the Governor of the Central Bank. In terms of section 31(1) of the *Payment System Bill, 2013*, "a person may not clear payment instructions unless the person is central bank settlement system participant; or bank, or branch of a foreign institution that is allowed to clear in terms of section 8 (3) (d) (i)."⁴⁵⁴ In terms of section 28 of the *Payment System Bill, 2013*, "a person may not participate in the central bank settlement system unless the person is the Central Bank, a bank, or a branch of a foreign institution and, in the case where the Body has been recognised by the Central Bank as contemplated in section 6, such person is a member of the Body so recognised."

⁴⁵⁵ See http://www.rbm.mw/documents/payment_systems/RTGS%20Access%20Criteria%20ofeb%202008.pdf

Reserve Requirement (LRR); and 4) they must maintain a Settlement Account with Reserve Bank of Malawi (previously called Current Account). Non-bank institutions must meet a number of applicable conditions. These are: 1) they must have an operating licence from the Reserve Bank of Malawi; 2) must maintain a current account with Reserve Bank of Malawi; 3) handle high value payments; and 4) their total payments must exceed 5% of the total industry value (mandatory).⁴⁵⁶ The Malawian Payment Systems Bill, 2014 contains several provisions on the licensing and authorisation of payment, clearing and settlement system operators, restrictions on the operation of payment systems or services, and authorisation requirements. The Bill does not however specify who may access and participate in settlement systems. The only reference to this is found in section 19 of the Bill which requires the Reserve Bank is to set minimum requirements for persons to participate in settlement systems it establishes, operates and controls. Section 19(2) empowers the Reserve Bank of Malawi to stipulate specific requirements in the form of directives or guidelines regarding the activities and security requirements applicable to settlement agents other than the Reserve Bank.

As Mauritius does not have a National Payment System Act / Payment System Management Act, access to and participation in the Mauritius Automated Clearing and Settlement System (MACSS) are only governed by Mauritius Automated Clearing and Settlement System Participant Procedures (Amended on 25 January 2013) and the MACSS Terms and Conditions. These documents are complimentary documents. The Mauritius Automated Clearing and Settlement System Participant Procedures do not specifically set out access or participation criteria, but Attachment F provides a list of participant bank identifier codes. 14 banks and the Bank of Mauritius are listed. Clause of 6.1 of the MACSS Terms and Conditions restricts participation in MACSS to institutions supervised by the Central Bank and licenced to undertake banking activities in Mauritius. The Central Bank is empowered to admit new participants at its sole discretion, always providing that such new participants be able and agree to comply with all the applicable requirements of the Terms and Conditions and the Procedures.

Article 3(1) of Mozambique's National Payment System Act, Law n° 2/2008 of 27 February lists the following as being subsystems of the payment system: real time gross settlement; settlement of transfer of funds and other financial assets; clearing houses for cheques, electronic payment orders, shares and negotiable instruments. Two provisions are contained in Mozambican Law n° 2/2008 of 27 February related to access and participation criteria for the settlement system. Article 19 that reads, "only entities with settlement accounts with the *Banco de Moçambique* may act as intermediaries in the transfer of funds for the settlement of payments." Article 21, which deals with central counterparties in financial transactions, states that, "with the approval of the *Banco de Moçambique*, participants in a payment subsystem, in compliance with the objective of public interest, may act as central or contractual counterparties for the purposes of settlement of obligations through the same payment subsystem." In addition, as per Article 21(2), "operators acting as central or contractual counterparties shall not be liable for the duty of payment of security for which the issuer is responsible." Notice n° 8/GBM/2009 of 23 December - Regulation Subsystem Transfer Clearance Wholesale Real Time / Real Time Metical (MTR), establishes the conditions for access / participation of institutions in the MTR.

In the Seychelles access to and participation in the settlement system is regulated by the National Clearance and Settlement Systems Act, 2010.⁴⁵⁷ In terms of section 4(c)(i) and section 4(c)(iv) of the National Clearance and Settlement Systems Act, 2010, the Central Bank will, on application, only recognise a clearance and settlement system if the rules or regulations governing the system are fair, equitable and transparent and make

⁴⁵⁶ Section 3.1 lists the following as following institutions are participants in the RTGS system: Reserve Bank of Malawi, National Bank of Malawi, Standard Bank of Malawi, First Merchant Bank, Loita Investment Bank, Nedbank, INDEbank Limited, Opportunity International Bank of Malawi, Continental Discount House, First Discount House, NBS Bank and the Malawi Savings Bank.

⁴⁵⁷ Act 12 of 2010.

adequate provision for admitting participants into the system and regulating and terminating their participation and criteria according to which a participant may be authorised to introduce any person to provide payment services. In terms of section 17(1) of the National Clearance and Settlement Systems Act, 2010, no person other than a participant in a recognised system or the Central Bank system, acting in accordance with the rules or regulations of the system or a person introduced by a participant in a recognised system or Central Bank system in accordance with a provision of the rules or regulations of the system, may, as a regular feature of the person's business, accept a transfer order from any person for the purposes of making a transfer on that other persons behalf. Unlike section 3(3)(a) of Botswana's National Clearance and Settlement Systems, 2003⁴⁵⁸, which states that the Central Bank will not recognise a clearance and settlement system unless it is satisfied that only financial institutions and the Central Bank are permitted to become participants in the system", the Seychelles National Clearance and Settlement Systems Act, 2010⁴⁵⁹ does not contain a provision of this kind. The Seychelles National Clearance and Settlement Systems Act, 2010 refers collectively to "clearance and settlement systems" and does not provide separate access and participation criteria for clearing systems and settlement systems.

Access and participation in the Swaziland Interbank Payment and Settlement System (SWIPSS) is regulated by the National Clearing and Settlement Systems Act, 2011.⁴⁶⁰ In terms of section 3(1)(b) of the National Clearing and Settlement Systems Act, 2011, the Central Bank may recognise a clearing and settlement system that has as its objectives the settling of obligations arising from the clearing and transfer instructions whether by (1) netting; (ii) set-offs; (iii) gross settlement.

As per section 3(3)(a) of Swaziland's National Clearing and Settlement Systems Act, 2011, the Central Bank will not recognise a clearing and settlement system unless it is satisfied that only financial institutions and the Central Bank are permitted to become participants in the system. Recognition will also only be granted as per section 3(3)(d) if the constitution and rules of the system are fair, equitable and transparent and make provision for –

- Admitting financial institutions into the system as participants and regulating and terminating their participation (section 3(3)(d)(i));
- Controlling the participants use of clearing and settlement systems and operations (section 3(3)(d)(ii));
- Criteria according to which a participant may be authorised to introduce any person to provide payment services (section 3(3)(d)(v)).

The definition of financial institutions as set out in section 2 of Swaziland's National Clearing and Settlement Systems Act, 2011 includes both a bank or any other financial institution which is licensed under the Financial Institutions Act, 2005 and a non-bank financial institution as defined in the Financial Services Regulatory Authority Act, 2010, therefore, access is open as per 3(3)(a) to institutions other than banks and the Central Bank in Swaziland. It is however recommended that Swaziland consider setting out concrete access and participation criteria as Namibia has done.

In the absence of a legally enforceable National Payment System Act, settlement system access and participation criteria in Tanzania are currently set out in the Tanzania Inter-Bank Settlement System Rules and Regulations.⁴⁶¹ Part II of the Rules sets out participation criteria and Part III, conditions and circumstances under

⁴⁵⁸ Act 5 of 2003.

⁴⁵⁹ Act 12 of 2010.

⁴⁶⁰ Act 17 of 2011.

⁴⁶¹ Available at: <https://www.bot-tz.org/PaymentSystem/TISS%20Rules%20and%20Regulations.pdf>

which participation may be withdrawn. In terms of Rule 11, participation in the TISS is open to a bank or financial institution or any participant provided it meets all the eligibility criteria and conditions as set out in the Tanzania Inter-Bank Settlement System Rules and Regulations. These are as follows:

- It has a settlement account at the Bank (Rule 11(a)),
- It meets the SWIFT connectivity requirements for domestic inter-bank settlement systems, which settle on both Real Time Gross Settlement and Deferred Settlement modes (Rule 11(b));
- It is capable of exchanging SWIFT authentication keys with all participants and any other components of the TISS necessary for proper authentication of messages (Rule 11(c));
- It has in the opinion of the Bank, appropriate technical capacity, including adequate contingency arrangements to enable it to participate in the TISS without hindering the TISS smooth operations (Rule 11(d));
- It has demonstrated and undertaken to ensure that in the event of problem with its system it shall be able to resume payment processing through the system within a period acceptable to the Bank (Rule 11(e));
- It has executed, and agrees to be irrevocably bound by the terms and conditions of the Agreement for Participating in TISS and these Rules and Regulations (Rule 11(f)).

In Zambia, section 5(2) of the National Payment Systems Act, 2007⁴⁶² permits the Bank of Zambia to designate a particular payment system as it considers necessary. Section 5(3)(a) of the Zambian National Payment Systems Act, 2007 in turn, permits the Bank of Zambia to regulate entry criteria of participants to a payment system. The National Payment Systems Act, 2007 is however silent on who may participate in a designated (settlement) system and on who may participate in a designated (clearing) system or whether such participant are required themselves to be designated.

Access and participation in the Zimbabwean Electronic Transfer and Settlement System (ZETSS) and the Clearing House is regulated by the Zimbabwean National Clearance and Settlement Systems Act, 2001.⁴⁶³ In terms of section 3(3)(a) of the National Clearance and Settlement Systems Act, 2001, the Reserve Bank will not recognise a payment system unless it is satisfied that only financial institutions and the Reserve Bank are permitted to become participants in the system.⁴⁶⁴ In addition, the Reserve Bank of Zimbabwe will not recognise a payment system unless the constitution and rules governing the system are fair, equitable and transparent and make adequate provision for admitting financial institutions into the system as participants and terminating their participation (section 3(3)(d)(i)), controlling its participants' use of payment, clearance or settlement systems or operations (section 3(3)(d)(ii)) and criteria according to which a participant may be authorised to introduce any person to provide payment services (section 3(3)(d)(v)).

In terms of section 3(4)(a) of the South African National Payments System Act, 1998⁴⁶⁵ only the following persons may participate in the Reserve Bank settlement system: the Reserve Bank; Banks or branches of foreign institutions;⁴⁶⁶ Mutual Banks;⁴⁶⁷ and Co-operative Banks.⁴⁶⁸

⁴⁶² Act 1 of 2007.

⁴⁶³ [Chapter 24:23].

⁴⁶⁴ Financial institution is defined in section 2 of the National Clearance and Settlement Systems Act, 2001 as "a banking institution registered in terms of the Banking Act [Chapter 24:20] or any other institution which lawfully engages in the banking activities specified in paragraphs (a), (d), and (f) of section seven of the Banking Act."

⁴⁶⁵ 78 of 1998 (As Amended).

⁴⁶⁶ Banks are registered under the Banks Act, 1990.

⁴⁶⁷ Mutual Banks are registered under the Mutual Banks Act, 1993 (As Amended).

⁴⁶⁸ Cooperative Banks are registered under the Cooperative Banks Act, 2007.

Each of these persons must be members of the Payments Association of South Africa (PASA)⁴⁶⁹, be designated system operators⁴⁷⁰ or meet the criteria for participation in the reserve Bank settlement system as established by the Reserve Bank in consultation with the payment system management body (PASA).⁴⁷¹

There are currently 23 participants in the SAMOS system. Banks which are not direct participants in SAMOS may use sponsorship arrangements through other qualifying banks to clear and settle on their behalf, or else to clear in their own name while achieving settlement through the sponsorship of a settlement bank.⁴⁷²

In terms of section 3(5) of the National Payments System Act, 1998 (As Amended), “no person may be allowed to clear as contemplated in section 4 (2) (d) (i) unless, in the case where a payment system management body has been recognised by the Reserve Bank as contemplated in subsection (1), such person is a member of the payment system management body so recognised.”

Section 4 (2) (d) in turn reads, “In addition to any other provisions thereof, the rules of the payment system management body must empower that body to recommend for approval by the Reserve Bank criteria subject to and in accordance with which a member that is also a Reserve Bank settlement system participant may be authorised to-

- (i) allow a bank, a mutual bank, a co-operative bank, a designated clearing system participant or branch of a foreign institution that is not a Reserve Bank settlement system participant to clear; or
- (ii) clear on behalf of a bank, a mutual bank, a co-operative bank, a designated clearing system participant or a branch of a foreign institution that is not a Reserve Bank settlement system participant: Provided that the member shall settle payment obligations on behalf of such bank, mutual bank, co-operative bank, designated clearing system participant or branch of a foreign institution referred to in subparagraphs (i) and (ii).”

The South African Reserve Bank’s position with respect to the different types of clearing arrangements that are acceptable within the National Payment System was issued in July 2007. Position Paper 01/2007 Bank Models in the National Payment System outlines various sponsorship arrangements that can be effected. Position Paper 02/2007 distinguishes between clearing and non-clearing banks as follows:

Non-clearing banks: these banks are regulated by the Registrar of Banks but are not settlement system participants as defined in the National payment System Act, 1998. These banks may not: 1) provide various payment services; 2) clear domestic payment instructions to or from other banks as a normal part of their business, may not operate a SAMOS account at the South African Reserve Bank and may not be members of PASA.

Clearing banks: these banks are regulated by the Registrar of Banks and are required to be members of PASA. These banks are settlement system participants and are therefore required to: 1) operate a SAMOS account at the South African Reserve Bank (unless operating by a sponsorship arrangement), 2) be a member of PASA, 3) be a member of one or more of the PCH participant groups, 4) provide to its clients one or more payment

⁴⁶⁹ Section 3(4)(a) National Payments System Act 78 of 1998 (As Amended).

⁴⁷⁰ Section 3(4)(b).

⁴⁷¹ Section 3(4)(c).

⁴⁷² Volker *Essential Guide to Payments: An Overview of the Services, Regulation and Inner Workings of the South African National Payment System* 227.

services defined in the position paper;⁴⁷³ 5) clear domestic payment instructions to and from other banks as a normal part of their business and 6) be a signatory to a clearing agreement and a member of a PCH.

Categories of clearing banks: Position Paper 01/2007 delineates clearing banks into different types. The Position Paper notes that within any specific Payment Clearing House (PCH), banks may select to operate in any of the following categories: direct clearing;⁴⁷⁴ sponsored clearing;⁴⁷⁵ mentored clearing;⁴⁷⁶ agency clearing;⁴⁷⁷ and technical outsourcing.⁴⁷⁸

As per paragraph 7, each bank is required to annually confirm its status as a clearing or non-clearing bank with the PASA before the 30th November each year. In addition, each bank is required to provide details of its participation in the various categories of clearing and any agency, sponsorship or mentorship arrangements.

After the Banking Enquiry Report of the Competition Commission was released, the South African Reserve Bank published Position Paper 02/2011 on Access to the National Payment System. This Position Paper makes it quite clear that the position of the South African Reserve Bank in 2011 was that, "only South African registered banks are allowed in the settlement domain. [...] Strict rules are applied, and these banks have to meet statutory and prudential requirements as set by the Registrar of Banks and the Bank. Furthermore, settlement participants must have the ability to meet the liquidity, information, communication, technology and security requirements set by the Bank to participate in the SAMOS environment."

However, in terms of Strategic Objective 1 of *Vision 2015*, the South African Reserve Bank is committed to continuing to evaluate and improve the participation of non-bank stakeholders in the clearing system and/or in formal payment system management structures. In order to achieve Strategic Objective 1, the promulgation of or amendments to existing legislation and or regulation is recognised as a critical success factor. The overall vision stated in *Vision 2015* is, "to maintain a world-class payment system that meets domestic, regional and international requirements." The primary strategic objectives are listed as follows:

⁴⁷³ Payment services are defined in paragraph 5.1 of *Position Paper 02/2007* as, "being the services whereby a bank enables its clients to (a) make third-party payments by providing its clients with the means to issue payments to the clients of another bank or the other bank itself, through direct access to their (the bank's clients') bank accounts; (b) receive payments directly into their (the bank's clients') accounts from clients of another bank or the other bank itself; (c) withdraw cash at another bank."

⁴⁷⁴ Direct clearing is the model in which a bank that provides all or some of the payment services defined in the Position Paper belongs to a particular PSH and participates in the particular PCH in its own right.

⁴⁷⁵ In a sponsored clearing model, a bank in a specific PCH provides some payment services but by virtue of an agreement with a direct clearing bank. The sponsored clearing bank's settlement obligations within the PCH are fulfilled by the sponsoring bank on behalf of the sponsored clearing bank.

⁴⁷⁶ Mentored clearing occurs where a new entrant bank in a particular PCH participates as a direct clearer but has a contractual agreement with another direct clearing bank for the purposes of guidance and assistance.

⁴⁷⁷ The Position Paper notes that, "Only a direct clearer may conclude an agency clearing arrangement with any other clearing bank in order to provide clearing services to the clients of the other bank via the practice of credit transfers. This means that facilities are offered to other clearing banks in order to allow clients of such other clearing banks to make deposits with such banks and to transfer the funds so deposited to the clients' banks. This service must be covered by a specific PCH agreement approved by PASA."

⁴⁷⁸ Technical outsourcing refers to the arrangement where a bank provides operational facilities to process payments or manage settlements for another participant bank in any PCH (or all PCHs) within any payment stream (or all payment streams). It is important to note however that the participating bank remains the principal for all clearing and settlement agreements into which it enters.

- Strategic Objective 1:** Continue to evaluate and improve the participation of non-bank stakeholders in the clearing system and/or in formal payment system management structures.
- Strategic Objective 2:** Enhance the oversight of banks and increase the focus on non-banks.
- Strategic Objective 3:** Enhance communication among stakeholders regarding National Payment System matters.
- Strategic Objective 4:** Enhance payment system human resources capacity in the broader National Payment System.
- Strategic Objective 5:** Ensure a high level of operational effectiveness of the payment system infrastructure.
- Strategic Objective 6:** Facilitate regional payment system infrastructure integration to meet the needs of the SADC region.
- Strategic Objective 7:** Formalise and implement the interchange determination process.

See Diagram J2 in Annexure J for a schematic representation of the access to the National Payment System National Payment System vision, fundamental principles, key strategies and critical success factors required for the successful execution of the access vision.⁴⁷⁹

It is important to note that the *Vision 2015* document specifically lists six categories of potential participants in the National Payment System. These are: Registered banks in terms of the South African banking legislation;⁴⁸⁰ qualifying non-banks that, subject to the discretion of the Bank, are designated to be clearing participants in terms of section 6 of the National Payment System Act; sponsored banks and non-banks that are designated by the Bank;⁴⁸¹ non-bank participants that include third-party service providers and system operators; non-banks that are allowed to issue payment instruments;⁴⁸² non-banks that issue prepaid instruments.⁴⁸³

Six strategies for increasing access to the National Payment System are presented in Vision 2015. Of particular relevance to this project are strategy 2) allow non-banks access to the National Payment System via directives; strategy 4) enhance entry criteria and other regulatory requirements for participants; strategy 6) introduce designation for different levels of non-bank participation in the National Payment System; strategy 7) amend legislation to enhance formal participation where required; and strategy 8) conclude MOUs between the NPSD and other sector specific regulators.

The Namibian Payment System Determination PSD-6 Criteria for Authorisation of Participants in the Clearing and Settlement Systems, 2013 became effective on the 31st August 2013. As per section 8.1, the Bank of

⁴⁷⁹ Langhan and Smith *The Legal and Regulatory Framework for Payments in 14 SADC Member States Volume II: Country Reports: South Africa Country Report* 160.

⁴⁸⁰ Only registered banks, qualifying in terms of the Bank's payment system criteria, are eligible to clear and settle in their own name in the books of the Bank.

⁴⁸¹ These banks and non-banks use sponsorship arrangements through other qualifying banks for clearing and settlement purposes. Sponsoring banks, subject to criteria for sponsorship, are required to ensure that obligations arising from the clearing of sponsored banks are settled.

⁴⁸² These payment instruments are linked to a credit line through which the non-banks provide credit to the public.

⁴⁸³ These payment instruments are non-encashable and can be used by the unbanked and banked public.

Namibia may designate a NBFi for the purposes of participating in clearing and settlement systems. The factors for such designation are set out as an example for other SADC Member States below.

The Bank of Namibia is required to consider the following factors:

- The actual or prospective participant must provide payment services and demonstrate its business need to clear and settle with other participants (section 8.4.1);⁴⁸⁴
- Such designation is in the public interest and is in the interest of promoting a NBFi that occupies a special position in a specific sector, particularly in prompting financial inclusion (section 8.4.2); and
- Any other matters the Bank considers relevant (section 8.4.3).

Eligibility for Authorisation: Only two categories of institutions are eligible for access to and participation in the clearing and settlement systems. These are:

- Registered banking institutions in terms of the Banking Institutions Act, 1998 (As Amended) (section 9.1.1); and
- Designated NBFis (section 9.1.2).

The criteria for access and participation in NISS are set out in section 11 of PSD-6. This section covers both direct and indirect participation. As the criteria are clear and precise, it is recommended that other SADC countries consider the adoption of criteria similar to those in Namibia, for access and participation in their clearing and settlement systems as an appropriate benchmark. The criteria as set out in section 11 are summarised in Table 39 below.

Table 39: Criteria for Access and Participation in NISS

Ref.	Criteria
Direct Access and Participation in NISS	
S11.1(a)	Be a Licensed or Registered Banking Institution or a Designated NBFi.
S11.1(b)	Participate in one or more of the Payment Clearing Houses (PCHs).
S11.1(c)	Hold a settlement account at the Bank subject to the provisions of section 33 of the Bank of Namibia Act 15 of 1997 (As Amended).
S11.1(d)	Must have signed the following bilateral agreements: (i) Master Repurchase Agreement (MRA) for intraday liquidity facilities and any other credit service as may be provided by the Bank; and (ii) An agreement showing connectivity to SWIFT.
S11.1(e)	Must have specialised skills and processing capabilities in settlement system operations.
S11.1(f)	Fulfill the participation requirements on an on-going basis.
S11.1(g)	Must have sufficient financial and capital resources to ensure the safe, efficient and ongoing

⁴⁸⁴ Payment services are defined as, “services enabling cash to be placed on a payment account and all of the operations required for operating a payment account. A service enabling cash withdrawals from a payment account and all of the operations required for operating a payment account. The execution of the following types of payment transactions: direct debits, including once-off direct debits; payment transactions executed through a payment card or similar device; credit transfers, including standing orders. The execution of the following types of payment transactions where the funds are covered by a credit line for the payment service user, direct debits, including once-off direct debits; payment transactions executed through a payment card or similar device; credit transfers, including standing orders, issuing payment instruments or acquiring payment transactions and money remittance.”

	participation in the settlement system.
S11.1(h)	Be able to comply with all settlement system technical, security and operational standards as determined by the payment system management body.
S11.1(i)	Be able to meet the financial criteria determined by the Bank from time to time.
Indirect Access and Participation in NISS	
S11.2(a)	Be a designated NBFi.
S11.2(b)	Be registered by and under the responsibility of the Direct Participant, acting on its behalf.
S11.2(c)	Have a contractual arrangement approved by the Bank with a Direct Participant incorporating a variety of risk-mitigating mechanisms ensuring that the Direct Participant protects the other participants from risks that might be introduced by such contractual arrangement.
S11.2(d)	Fulfill the participation requirements on an on-going basis.

Application Procedure for Designation: Section 12 of PSD-6 clearly sets out the application procedures for any NBFi wishing to access and participate in the clearing and settlement systems in Namibia. In terms of section 12.1, applications by NBFis for designation must be made directly to the Bank of Namibia and consist of the documents set out in Table 40 below.

Table 40: Documents to be provided by NBFis Applying for Designation

Ref.	Information required for Designation
Designation	
S12.1.1	An application accompanied by a non-refundable application fee. ⁴⁸⁵
S12.1.2	MOA
S12.1.3	Applicant’s financial statements and its policies and strategies relating to the future development of its provision of payment services.
S12.1.4	The details of the proposed directors, officer and shareholders of the applicant.
S12.1.5	The structure and shareholding of the group of companies of which the applicant forms a part or intends to form a part.
S12.1.6	The integrity of the applicant and its competence to provide, or experience in providing payment services.
S12.1.7	Detailed proposed business plan / strategic plan including a forecast budget calculation for the first three financial years related to the business operations.
S12.1.8	Identity of Auditors.
S12.1.9	Address of the applicant’s Head Office.

Authorisation: In terms of section 12.2 of PSD-6, persons who wish to access and participate in the clearing and settlement systems are required to submit an application to the Bank of Namibia for authorisation and must fulfill the requirements set out in sections 9⁴⁸⁶, 10⁴⁸⁷ and 11.⁴⁸⁸

⁴⁸⁵ Section 13 sets out the fees payable to the Bank of Namibia. In terms of section 13.1, for an application for designation, a non-refundable application fee at the time of application of N\$10 000 is payable together with an annual renewal fee of N\$5000. Section 13.2 states that, “for an application for authorisation to participate in the clearing and settlement systems, no fee is payable. However user fees are payable and shall be prescribed by the respective providers of the clearing and settlement services.”

⁴⁸⁶ Section 9 – Eligibility for Authorisation.

⁴⁸⁷ Section 10 – Criteria for Access and Participation in Clearing Systems.

⁴⁸⁸ Section 11 – Criteria for Access and Participation in the Settlement System.

Authorisation may, in terms of section 15 of PSD-6 be cancelled by the Bank of Namibia if:

- The person fails to comply with PSD-6 and remedial measures required by the Bank following inspection (section 15.1.1);
- It is determined that an authorisation was obtained on the strength of misrepresented, inaccurate, or misleading information furnished to the Bank of Namibia at the time of application (section 15.1.2);
- There is a violation of any of the provisions of PSD-6, the Payment System Management Act, 2003 (As Amended) and any other applicable law or regulations (section 15.1.3);
- The person ceases to operate or becomes insolvent (section 15.1.4);
- Any other circumstances which the Bank may consider material to warrant cancellation (section 15.1.5).⁴⁸⁹

5.6 Settlement Finality and Irrevocability

Legal certainty as to the effectiveness of transfers of funds and securities is a prerequisite for establishing market confidence, fostering the protection of investors and limiting risk in the financial markets. Of particular relevance in the context of the legal protection of market infrastructures is the concept of settlement finality and irrevocability.⁴⁹⁰ Finality is important because when it occurs, as set out in the laws, regulations and rules applicable in each country, the obligations generated in the interbank payment, clearing and settlement process are discharged. Therefore, the credit, liquidity and systemic risks generated as part of this process cease to exist at this point in time. As a result, finality is the most important concept in the analysis of the credit, liquidity and systemic risks in payment and settlement systems.⁴⁹¹

Over the years, finality has increasingly been associated with the reduction of insolvency-related risks resulting from participation in payment, clearing and settlement systems. In recognition of this, in 1998 the European Union adopted the Settlement Finality Directive 98/26/EC (As Amended by Directive 2009/44/EC. This Directive applies to systems designated by their national authorities as being covered by it and created an EU-wide legal framework to reduce systemic risk linked to payment, clearing and settlement systems and protect systems and their participants against the adverse effects of insolvency proceedings opened against another system participant.⁴⁹²

Two of the principles set out in the *Principles for Financial Market Infrastructures (PFMI)*⁴⁹³ report are particularly relevant in this regard. They are: Principle 8 Settlement Finality and Principle 9 Money Settlements. Principle 8 requires that an FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time. Principle 9 requires that an FMI should conduct its money settlements in central bank money where practical and

⁴⁸⁹ In terms of section 15.1.6, the Bank of Namibia is required to ensure that all due diligence processes are followed before cancellation of an authorisation to access and participate in the clearing and settlement systems.

⁴⁹⁰ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 144.

⁴⁹¹ 145.

⁴⁹² The Directive aims to reduce the systemic risk associated with participation in payment and securities settlement systems ("systems"), and in particular the risk linked to the insolvency of a participant in such a system. To this end, it lays down common rules stipulating that: transfer orders and netting must be legally enforceable; transfer orders may not be revoked once they have been entered into the system; the insolvency of a participant may not have retroactive effects; the insolvency law applicable is the law of the Member State whose system is involved.

⁴⁹³ Bank for International Settlements and International Organization of Securities Commissions *Principles for Financial Market Infrastructures (PFMI)*.

available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money. As can be seen in Table 41 below, the current National Payment System Act in force in several SADC Member States does not contain a provision requiring that money settlements be effected in Central Bank Money.

Table 41: PFMI's 8 and 9

	ANG	BWA	DRC	LSO	MW	MU	MOZ	NA	SC	RSA	SW	TZ	ZM	ZW
PFMI's 8 and 9														
Principle 8: An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.	✓	✓	●	●	●	* 494	✓	✓	✓	✓	✓	* 495	✓	✓
Principle 9: An FMI should conduct its money settlements in central bank money where practical and available	✓	✗	✗	●	●	* 496	✓	✓	✗	✓	✗	* 497	✓	✗

An additional area of concern is that provisions on settlement finality and irrevocability and money settlements in central bank money are not included in Mauritian Law or Regulations. This is an area of great concern as the only references to finality and irrevocability are found in the *Port Louis Automated Clearing House Rules* and the *Mauritius Automated Clearing and Settlement System Terms and Conditions*. The reliance on these bi-lateral arrangements between participants' results in an ad-hoc self-regulated payments industry, a situation that should not be left unchecked by the Central Bank. As the payment system is maturing in Mauritius, it is vital that legislation in the form of a National Payment System Act is introduced so as to allow for more formalised regulation.⁴⁹⁸ The same can be said for the DRC, Lesotho, Malawi and Tanzania that have yet to pass their National Payment System Bills.

5.7 Transfer Orders and Netting

The Settlement Finality Directive (As Amended) ensures that netting is legally enforceable and binding on third parties even in the event of insolvency proceedings and precludes the application of zero-hour rules.⁴⁹⁹

⁴⁹⁴ See Port Louis Automated Clearing House Rules and Mauritius Automated Clearing and Settlement System Terms and Conditions.

⁴⁹⁵ Provisions on settlement finality and irrevocability and money settlements in central bank money are not currently included in a legally enforceable statute in Tanzania. This is an area of concern as the only references to finality and irrevocability are found in the Tanzania Inter-Bank Settlement System Rules and Regulations. It has however been stated by the Bank of Tanzania that, "TISS complies with both principles 8 and 9 of the PFMI's with basis on the laws of general application which has been reflected in the proposed National Payment Systems Act. See Rule 4 and Rule 29 of the Tanzania Inter-Bank Settlement System Rules and Regulations.

⁴⁹⁶ See Mauritius Automated Clearing and Settlement System Terms and Conditions.

⁴⁹⁷ See Rule 11(a) and Rule 41(1) of the Tanzania Inter-Bank Settlement System Rules and Regulations.

⁴⁹⁸ See Volker *Essential Guide to Payments: An Overview of the Services, Regulation and Inner Workings of the South African National Payment System*.

⁴⁹⁹ Netting is defined as the determination of the net payment obligations between two or more clearing system participants within a payment clearing house or the determination of the net settlement obligations between two or more

5.7.1 Transfer Orders and Netting Are Legally Enforceable and Binding on Third Parties

Article 3(1) of the Settlement Finality Directive (As Amended) provides that, "Transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, **provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings.** This shall apply even in the event of insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system who is not a participant. Where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties **only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.**

When compared to the provisions found in the National Payment System Act or Bill in each SADC Member State, the domestic provisions are found to be lacking in a number of respects. A discussion of each country's approach and the comparative shortfalls in the legal text is set out below.

Article 20 of the Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems is the only article in the Law that refers to insolvency. This article reads,

"(1) Bankruptcy or operating regime under exceptional or insolvency conditions, to which a participant is subject, does not produce any effect with regard to settlement obligations and receiving rights of participants whose operations have had a final settlement or have been accepted by the subsystem or clearing houses before such regime was decreed.

(2) In relation to a participant subject to the situation referred to in the previous number, the product from the execution of guarantees made to subsystems or clearing houses by the participant, as well as the securities, subject of negotiation in the execution of guarantees, shall be intended for the settlement of the obligations undertaken by the participant in the said subsystem or clearing houses."

Section IV of the Act specifically covers multilateral netting that is defined in Article 18 as, "the procedure for determining each participant's balance by summing up the debtors and creditors' bilateral balances of each in relation to the other." Article 19 sets out the mechanism for the settlement of multilateral netting and provides that clearing house regulations may provide for the opening of an account with the Central Bank in the name of the operator thereof, as a settlement mechanism for the operations undertaken or settled through the account (Article 19(1))" As per Article 19(2), "the account in the name of the chamber should not generate a balance different from zero after the daily closing of the final settlement of the operations processed therein."

While Articles 18 and 19 of Law nº 5/05 Dated July 29 refer to multilateral netting, Article 20 that covers insolvency makes no direct reference to the legal enforceability of transfer orders or netting, although upon the normal interpretation of Article 20 this may be inferred. It is however important to note that the Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems does not state that "transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a

settlement participants within a settlement system. The zero-hour rule is a provision in the insolvency law of some countries whereby the transactions conducted by an insolvent institution after midnight on the date the institution is declared insolvent are automatically ineffective by operation of law.

participant, **provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings.**" Although the moment of "payment finality" is defined in Articles 22 and 24, the **moment of the opening of insolvency proceedings** is not mentioned nor defined. Law nº 5/05 Dated July 29 Law of Angolan Payment Systems is also deficient in a number of other respects including, no reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and no provision covering the situation where "transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

It is also important to highlight that Law nº 5/05 Dated July 29 Law of Angolan Payment Systems specifies that the **rules** of a payment system must specify **the moment** at which a transfer order shall be considered to have been entered into the payment system. As per Article 23, the timeframe and responsibilities for the finalisation of payment must be established in the subsystem or chamber's regulations and disclosed to the public. Similarly, Article 24(2) that refers to situations where payments are not settled through subsystems or chambers, requires the timeframe for the finalisation of payments to be established in the procedures governing the provision of the service and to be disclosed to the users of such service.

Section 14 of Botswana's National Clearance and Settlement Systems Act, 2003⁵⁰⁰ reads, "notwithstanding anything to the contrary in the Insolvency Act, or the Companies Act, where a participant in a recognised system- (a) is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act; or (b) is placed under curatorship in terms of the Banking Act, any provision relating to clearance or settlement to which the participant is a party shall be binding upon the participant's liquidator, judicial manager, provisional judicial manager or curator, as the case may be. (2) Subsection (1) shall apply to the extent that it applies to any payment obligation or settlement obligation which- (a) was determined through clearance or settlement before the issue of the winding up order or the order placing the participant under judicial management, provisional judicial management or curatorship, as the case may be; and (b) was either- (i) to be discharged or transferred on or after the issue of that order; or (ii) was overdue for settlement on the date of that order."

When Article 3(1) of the Settlement Finality Directive (As Amended) is compared to section 14 of Botswana's National Clearance and Settlement Systems Act, 2003 it is clear that Botswana's Act does not specifically refer to "transfer orders and netting" but rather to "payment or settlement obligations". While netting is inferred by reading section 3(1)(b) together with section 14, it would be preferable to use wording such as "transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings." Section 14 of the National Clearance and Settlement Systems Act, 2003 does not contain any reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and does not provide for "where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

⁵⁰⁰ Act 5 of 2003.

The DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 contains three provisions in this regard. Article 6 and Article 7 (as set out in Table 11 above) and Article 14 are mostly compliant with Article 3(1) of the Settlement Finality Directive (As Amended) although Articles 6, 7 and 14 do not refer to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and does not provide for "where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings." Article 14 also appears to be placed in the wrong section of the Draft Law and should be grouped with Articles 6 and 7.

Part V of the Lesotho's National Payment Systems Bill, 2013 covers insolvency. Article 17 reads,

"(1) Nothing in the Insolvency Proclamation of 1957 shall invalidate or affect the rights and obligations of any participant in respect of any transaction made 6 months prior to the issuance of an insolvency order against any participant in terms of this Act.

(2) The following are valid, enforceable and binding against the liquidator or third parties:

(a) Cash or securities transfer orders and the payments resulting from such transfer orders, which have been entered into the system in accordance with its rules prior to the issuance of an insolvency order; and

(b) The netting of cash or securities transfer orders and of the debts and obligations resulting from such transfer orders when the former have been entered into a system in accordance with its rules prior to the issuance of an insolvency order.

(3) A transfer order entered into a system shall not be revoked by a participant in the system, nor by any third party, including the liquidator, from the moment defined by the rules of that system.

(4) Notwithstanding the event of insolvency against a participant in a system, the operator of the system or the settlement agent may, if it is so authorised under the applicable contractual provisions, make use of funds and financial instruments available on the settlement account of the participant in order to settle outstanding transfer orders and any net debit balance the participant may owe after netting, thus allowing for final settlement of the system.

(5) For the purpose of subsection (4) and notwithstanding the event of insolvency against a participant in a system, the operator of the system or the settlement agent is also authorised, subject to section 31, and under the applicable contractual conditions, to make use of credit lines granted to the participant and to realise any collateral provided with the aim to secure such credit lines."

It is unclear why Lesotho has elected to refer to "transaction made 6 months prior to the issuance of an insolvency order against any participant" rather than just "**transfer orders entered into the system before the moment of opening of such insolvency proceedings.**" The critical element is the requirement to define the moment of the opening of insolvency proceedings, not the time period before the opening of such proceedings. Lesotho's National Payment Systems Bill, 2013 does not define the "moment of the opening of insolvency proceedings. Section 17 is also deficient in that it does not contain any reference to "insolvency

proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant” and does not provide for “where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.”

Part V of the Malawian Payment Systems Bill 2014 covers both netting and financial collateral arrangements. As per section 29(2), “where a clearing or settlement system participant is wound up or placed under receivership or statutory , any arrangement or provision contained in any written netting agreement to which such a system participant is a party, or any netting rules and practices applicable to such a system participant, shall be binding upon the liquidator, receiver or statutory manager as the case may be in respect of any payment or settlement obligation,

- (a) which has been determined through netting prior to the issue of the winding-up order, receivership order or appointment of a statutory manager as the case may be;
- (b) which is to be discharged on or after the date of the winding up-order, receivership order or appointment of the statutory manager as the case may be; or
- (c) the discharge of which was overdue on the date of winding-up order, receivership order or the appointment of the statutory manager as the case may be.”

If these two provisions are compared, section 29(2) of the Malawian Payment Systems Bill, 2014 while more comprehensive than most provisions found in other SADC member States Acts, does not contain any reference to “insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant” and does not provide for “where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.”

As Mauritius has not enacted a National Payment System Act, one has to search for relevant provisions in other law and regulation. As noted by the Bank of Mauritius in a presentation to the CMA Payment System Integration Workshop held in Pretoria in 2011, “The Bank of Mauritius realising the potential difficulties created by the zero-hour-rule added a definition of real time gross settlement to the MACSS contracts so as to circumvent such difficulties.”⁵⁰¹ The definition added is as follows, “Real-Time Gross Settlement means the processing and settlement of payment obligations in real time on a gross basis. To the extent it is permissible by law the parties agree that for the purposes of the present agreement and all settlements performed thereunder, a day shall be reckoned as being a 24-hour period, starting from the real time of a transaction to end a second prior to the 24th hour immediately following that transaction and that each second, minute and hour over a day shall be deemed to occur in succession and in the real order in which they develop.” While this is a useful definition we maintain that it is not sufficient to “circumvent” the difficulties caused by not having a legally enforceable provision such as Article 3(1) of the Settlement Finality Directive (As Amended) in Mauritian Law.

⁵⁰¹ See Bank of Mauritius (2011) *Legal Framework of the Domestic Payment System of Mauritius* .

An additional measure taken by Mauritius was to amend the Insolvency Act, 2009⁵⁰² by inserting section 410 into the law. Section 410 of the Insolvency Act, 2009 (As Amended) reads, "Notwithstanding any other enactment where (a) a person is adjudicated bankrupt; or (b) a company is wound up, any payment, settlement or transaction shall have effect having regard to the time at which the Official Receiver or liquidator is appointed as recorded on the bankruptcy order in the case of bankruptcy and as required to be recorded in the case of a company winding up."

If compared with Article 3(1) of the Settlement Finality Directive (As Amended), Section 410 of the Insolvency Act, 2009 (As Amended) is deficient in a number of respects. Section 401 of the Insolvency Act, 2009 (As Amended) does not contain any reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and does not provide for "where transfer orders are entered into a system **after the moment of opening of insolvency** proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

Article 16 of the Mozambican Law 02/08 of 27 February is the only article in the Law that refers to insolvency. Article 16 reads, "Bankruptcy, insolvency, financial restructuring, extrajudicial liquidation or similar procedures brought against any participant shall not affect such participant's duty to comply with obligations assumed within the ambit of payment subsystems, which shall be settled in the terms and conditions set out in this Law and regulations approved for its implementation." *Multilateral clearing* is covered by Articles 22 and 23 of the Act. Article 22 reads, "for the purposes of settling financial obligations, the multilateral clearing of obligations in the same payment subsystem shall be permitted." Article 23 of Law 02/08 sets out the "mechanism for the settlement of multilateral clearing"⁵⁰³ and permits operators of payment subsystems to hold settlement accounts in the name of the respective operator with the *Banco de Moçambique*, for purposes of settling operations under the terms and conditions established by the *Banco de Moçambique*.⁵⁰⁴

Neither of these provisions refers directly to transfer orders and netting, neither do they state that "transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, **provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings.**" Although the moment of "payment finality" is defined in Article 13 of Law 02/08 of 27 February, the moment of the opening of insolvency proceedings is not mentioned nor defined. Law 02/08 of 27 February is also deficient in a number of other respects including, no reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and no provision covering the situation where "transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

It is also important to highlight that Law 02/08 of 27 February does not specify that the **rules** of a payment system must specify **the moment** at which a transfer order shall be considered to have been entered into the

⁵⁰² Act 3 of 2009.

⁵⁰³ This wording is extracted directly from the Law.

⁵⁰⁴ Article 23(2) of Law 02/08 reads, "the balance in the account referred to in the paragraph above [Article 23(1)] shall be zero at the daily close of the final settlement of operations processed through such account."

payment system although Article 13(3) requires that “the regulations covering each payment subsystem shall specify the time period and the consequences of the failure to reach payment finality.” Article 13(3) is very broadly drafted and it will be difficult for the layman to interpret what “time period” the Article is referring to.

Part III of the Seychelles National Clearance and Settlement Systems Act, 2010⁵⁰⁵ consists of two sections and covers the finality of payments and transfers (section 11) and the utilization of deposits (section 12). Section 11 of the National Clearance and Settlement Systems Act, 2010 is comprehensive and is the closest in terms of content and structure to Article 3 of the Settlement Finality Directive (As Amended). It is important to note that while it appears that the Zimbabwe and Botswana National Clearance and Settlement Systems Acts were drawn heavily upon by the drafters of the Seychelles Act, section 11 of the Seychelles National Clearance and Settlement Systems, 2010 is unique to the Seychelles differs substantially from the provisions found in Zimbabwe and Botswana’s Acts.

Sections 11(1) and 11(2) of the Seychelles National Clearance and Settlement Systems Act, 2010 read, “1) Notwithstanding any other written law to the contrary, a payment or transfer instruction which is entered into a recognised system or the Central Bank System shall be legally enforceable and binding on third parties, notwithstanding the commencement of winding up of the participant or placing the participant under receivership, provided that the payment or transfer instruction was entered into the recognised system or the Central Bank system, as the case may be, prior to the commencement of the winding up of the participant or placing of the participant under receivership.

(2) Where a payment or transfer instruction has been entered into a recognised system or the Central Bank system after the commencement of the winding up of the participant or placing the participant under receivership the payment or transfer instruction shall be legally enforceable and binding on third parties only if, after the time of settlement, the management body or the Central Bank system, as the case may be, can prove that it was not aware nor should have been aware of the commencement of the winding up of the participant or placing of the participant under receivership, as the case may be.”

The only wording that is not included in the text of sections 11(1) and (2) of the Seychelles National Clearance and Settlement Systems Act, 2010 is, “this shall apply even in the event of insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant.” It is recommended that the Seychelles consider amending section 11(1) by inserting these words.”

Section 11(3) of the Seychelles National Clearance and Settlement Systems Act, 2010, unlike most National Payment System Acts in force in other SADC countries specifically states that, “the moment of entry of a payment or transfer instruction in a recognised system or the Central bank system shall be determined by the rules of the system.” What the Act does not provide for however is a concrete definition of the **moment of the opening of insolvency proceedings**. It is recommended that this deficiency be resolved as soon as is reasonably practicable.

Article 8(2) of the South African National Payments System Act, 1998 (As Amended)⁵⁰⁶ reads, “if a curator of similar official is appointed to a clearing system participant or a settlement system participant, the curator or similar official is bound by any –

⁵⁰⁵ Act 12 of 2010.

⁵⁰⁶ Act 78 of 1998 (As Amended).

- (a) provision contained in the settlement rules or in clearing, netting and settlement agreements to which that clearing system participant or settlement system participant is a party, or any rules and practices applicable to the clearing system participant or settlement system participant in relation to such agreement; and
- (b) payment or settlement that is final and irrevocable in terms of section 5(2) or (3).⁵⁰⁷

Section 8(6) of the South African National Payments System Act, 1998 (As Amended) covers the situation where a clearing or settlement system participant is wound-up. In this case, as in the case where a curator or similar official is appointed to a clearing system participant or a settlement system participant, the liquidator or similar official is also bound by provision contained in the settlement rules or in clearing, netting and settlement agreements to which that clearing system participant or settlement system participant is a party, or any rules and practices applicable to the clearing system participant or settlement system participant in relation to such agreement.⁵⁰⁸

If the two provisions in the South African National Payment System Act 1998 (As Amended) are compared to Article 3(1) of the Settlement Finality Directive (As Amended) the South African National Payments System Act, 1998 (As Amended) refers to the "provisions contained in the settlement rules or in clearing, netting and settlement agreements to which that clearing system participant or settlement system participant is a party." While it is quite conceivable that such rules or agreements contain rules and clauses that have the effect of making transfer orders and netting legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, **provided that transfer orders were entered into the system before the moment of opening of insolvency proceedings**, the National Payment System Act, 1998 (As Amended) itself is silent on this matter. It is also essential that the moment of opening of insolvency proceeding is adequately defined in the law (see section 2.3.7 below.) This is not the case in the National Payment System Act, 1998 (As Amended) and reviewing all of the netting and settlement agreements applicable in the South African context is out of the scope of this review. It is also important to note that the National Payments System Act, 1998 (As Amended) does not contain any reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and does not provide for "where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

As provisions covering transfer orders and netting should preferably be contained in legislation rather than contract or multilateral agreement or rules, it is recommended that the South African Reserve Bank consider amending section 8(2) of the National Payment System Act, 1998 (As Amended).

⁵⁰⁷ In the case of a curator having been appointed, such curator may (at his discretion) give written notice to the Reserve Bank to withdraw such participant's participation in the clearing system or the Reserve Bank settlement system (section 8(3)).

⁵⁰⁸ In the case where a clearing system participant or settlement system participant is wound-up and in respect of whom a copy of the winding-up order has been lodged with the Reserve Bank, such participant must not, as set out in section 8(7) be entitled to clear or participate in any settlement system, other than for the purpose of discharging payment or settlement obligations in accordance with the rules of the settlement system or clearing, netting and settlement agreements to which the clearing system participant or settlement system participant is a party, or any rules and practices applicable to the clearing system participant or the settlement system participant in relation to such agreements.

Section 14 of Swaziland's National Clearing and Settlement Systems Act, 2011⁵⁰⁹ reads, "Notwithstanding anything to the contrary in the Insolvency Act, 1955, or the Companies Act, 1912, where a participant in a recognised or Central Bank system (a) is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act, 2009 or (b) is placed under curatorship in terms of the Financial Institutions Act, 2005, any provision relating to clearance or settlement to which the participant is a party shall be binding upon the liquidator, judicial manager, provisional judicial manager or curator of the participant, as the case may be to the extent that it applies to any payment obligation or settlement obligation which (i) was determined through clearing or settlement before the issue of the winding up order or the order placing the participant under judicial management, provisional judicial management or curatorship, as the case may be; and (ii) was either to be discharged or transferred on or after the issue of that order; or was overdue for settlement on the date of that order."

If section 14 of Swaziland's National Clearing and Settlement Systems Act, 2011 is compared to Article 3(1) of the Settlement Finality Directive (As Amended) it is clear that the Swaziland provision does not specifically refer to "transfer orders and netting" but rather to "clearance or settlement obligations". While netting is inferred by reading section 3(1)(b) together with section 14 of the National Clearing and Settlement Systems Act, 2011, it would be preferable to use wording such as "transfer orders and netting shall be legally enforceable and binding on third parties even in the event of insolvency proceedings against a participant, provided that transfer orders were entered into the system before the moment of opening of such insolvency proceedings." Section 14 of Swaziland's National Clearing and Settlement Systems Act, 2011 does not contain any reference to "insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant" and does not provide for "where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings."

As Tanzania has not enacted a National Payment System Act, one has to search for relevant provisions in other laws, regulations and rules. It is noted that the Bank of Tanzania Act, 2006⁵¹⁰ does not contain any provisions on transfer orders and netting nor do the Tanzania Inter-Bank Settlement System Rules and Regulations contain any legally enforceable provision covering the subject matter of Article 3(1) of the Settlement Finality Directive (As Amended).

Section 25 of the Zambian National Payment Systems Act, 2007⁵¹¹ reads,

"(1) this section shall apply to participants notwithstanding any other law to the contrary.

(2) Where a participant is wound up, placed under receivership or a curator is appointed, any provision contained in a written agreement to which the participant is a party or any netting rules applicable to that participant shall be binding upon the liquidator, receiver or curator, as the case may be, in respect of any payment or settlement obligation –

(a) which has been determined through netting prior to the issue of the winding-up or receivership order or the appointment of the curator; and

(b) which is to be discharged on or after the date and minute in the hour of the winding-up or receivership order or the appointment of the curator, the discharge of which was overdue on the date and minute in the hour of the winding-up or receivership order or the appointment of the curator."

⁵⁰⁹ Act 17 of 2011.

⁵¹⁰ Act 4 of 2006.

⁵¹¹ Act 1 of 2007.

If section 25 of the *Zambian National Payment Systems Act, 2007* is compared with Article 3(1) of the *Settlement Finality Directive*, while the Zambian provision is better than most found in the *National Payment System law* in other SADC countries, it does not contain any reference to “insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant” and does not provide for “where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.”

It is also important to highlight that while section 17 of the *National Payment System Act, 2007* covers the validity of clearing house rules, the section does not specify that the rules of a payment system must specify **the moment** at which a transfer order shall be considered to have been entered into the payment system.

Section 15 of Zimbabwe’s *National Payment Systems Act [Chapter 24:23]* reads, “Notwithstanding anything to the contrary in the *Insolvency Act [Chapter 6:04]* or the *Companies Act [Chapter 24:03]*, where a participant in a recognised payment system (a) is wound up or placed under judicial management or provisional judicial management in terms of the *Companies Act [Chapter 24:03]* or (b) is placed under curatorship in terms of the *Banking Act [Chapter 24:20]*, any provision relating to netting or settlement which is contained in the constitution or rules of the system concerned or in any agreement to which the participant is a party shall be binding upon the participant’s liquidator, judicial manager, provisional judicial manager or curator of the participant, as the case may be to the extent that it applies to any payment obligation or settlement obligation which (i) was determined through netting or settlement before the issue of the winding up order or the order placing the participant under judicial management, provisional judicial management or curatorship, as the case may be; and (ii) was either to be discharged or transferred on or after the issue of that order; or was overdue for settlement on the date of that order.”

If section 15 of the *Zimbabwean National Payment Systems Act [Chapter 24:23]* is compared to Article 3(1) of the *Settlement Finality Directive (As Amended)* the Zimbabwean provision does not contain any reference to “insolvency proceedings against a participant (in the system concerned or in an interoperable system) or against the system operator of an interoperable system which is not a participant” and does not provide for “where transfer orders are entered into a system after the moment of opening of insolvency proceedings and are carried out within the business day, as defined by the rules of the system, during which the opening of such proceedings occur, they shall be legally enforceable and binding on third parties only if the system operator can prove that, at the time that such transfer orders become irrevocable, it was neither aware, nor should have been aware, of the opening of such proceedings.”

It is also important to highlight that several Acts and Bills do not specify that the rules of a payment system must specify **the moment** at which a transfer order shall be considered to have been entered into the payment system.

5.7.2 No Law, Regulation or Rule Will Result in the Unwinding of Netting

Article 3(2) of the Settlement Finality Directive (As Amended) reads, “No law, regulation, rule or practice on the setting aside of contracts and transactions concluded before the moment of opening of insolvency proceedings, as defined in Article 6(1) shall lead to the unwinding of a netting.”

The Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems, *the DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013* do not contain a provision of this nature.

Section 13 of Botswana’s National Clearance and Settlement Systems Act, 2003⁵¹² reads, “notwithstanding anything to the contrary in the Insolvency Act or the Companies Act, the winding up of a participant in a recognised system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section 10 before the copy of the relevant order was lodged with the Central Bank in terms of section 14.” The reference to these two laws only limits the scope of the provision. It is therefore suggested that specific laws are not named by rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered.

Section 17 of Lesotho’s National Payment System Bill, 2013 makes specific reference to the Insolvency Proclamation, 1957⁵¹³ only. The reference to this ordinance only limits the scope of the provision and it is therefore recommended that Lesotho consider not naming specific laws but rather rewording this section with a broader provision such as, “no law, regulation, rule or practice on the setting aside of contracts and transaction shall...”

The Malawian National Payment Systems Bill, 2014 is compliant in this regard. It is also important to note that the drafters of the Bill have not limited the application of section 25 to just the provisions found in the Banking Act, Financial Services Act, Companies Act or Bankruptcy Act as the use of the words, “and any other written law in Malawi” creates a “catch all” situation.

Section 401 of the Mauritian Insolvency Act, 2009 (As Amended) does refer to “any other enactment” but does not make direct reference to the “unwinding of a netting”, although this may be implied by the use of the words “payment, settlement or transaction” which are potentially broad enough to included netted transactions.

The Mozambican Law 02/08 of 27 February does not contain a provision such as this.

Section 8 of the Namibian Payment System Management Act, 2003 (As Amended)⁵¹⁴ makes specific reference to the Insolvency Act or the Banking Institutions Act. The reference to these two laws only limits the scope of the provision. It is therefore suggested that specific laws are not named by rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered.

Section 14 of the Seychelles National Clearance and Settlement Systems Act, 2010⁵¹⁵ is drafted in a different form but has the same effect as Article 3(2) of the Settlement Finality Directive (As Amended).⁵¹⁶ Once again,

⁵¹² Act 5 of 2003.

⁵¹³ No. 51 of 1957.

⁵¹⁴ Act 18 of 2003 (As Amended).

⁵¹⁵ Act 12 of 2010.

the only deficiency identified is the lack of a definition on the **moment of the opening of insolvency proceedings**.

Section 8(1) of the South African National Payments System Act, 1998 (As Amended)⁵¹⁷ reads, “The provisions of this section apply despite anything to the contrary in the laws relating to insolvency or in the Companies Act, the Banks Act, the Cooperative Banks Act, the Postal Services Act, 1998 (Act 124 of 1998) or the Mutual Banks Act.” Section 8(1) refers to all the provisions contained in section 8, which by reference includes section 8(2)(a)). However, once again, the fact the “moment of opening of insolvency proceedings is not defined in the National Payment System Act is cited as a deficiency in the National Payment System Act. The reference to specific acts also limits the application of the provision to these specific acts. It is therefore suggested that specific laws are not named by rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered.

Section 13 of Swaziland’s National Clearing and Settlement Systems Act, 2011 reads, “notwithstanding anything to the contrary in the Insolvency Act, 1955 or the Companies Act, 2009, the winding up of a participant in a recognised or Central Bank system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section 10 before the copy of the relevant order was lodged with the Central Bank in terms of section 12.” The reference to these two laws only limits the scope of the provision. It is therefore suggested that specific laws are not named by rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered.

It is noted that the Bank of Tanzania Act, 2006⁵¹⁸ does not contain such a provisions nor do the Tanzania Inter-Bank Settlement System Rules and Regulations contain any legally enforceable provision covering the subject matter of Article 3(2) of the Settlement Finality Directive (As Amended).

Section 25 of the Zambian National Payment Systems Act, 2007⁵¹⁹ is drafted very broadly and refers to “any other law to the contrary.” This is in contrast to most National Payment System Acts in the region that refer specifically to the Insolvency Act, Financial Services Act of Company Act. The provision in the Zambian law is preferred.

Section 14 of the Zimbabwean National Payment Systems Act [Chapter 24:23] reads, “notwithstanding anything to the contrary in the Insolvency Act [Chapter 6:04] or the Companies Act [Chapter 24:03], the winding up of a participant in a recognised payment system or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment

⁵¹⁶ Section 14 of Act 12 of 2010 reads, “notwithstanding any other written law to the contrary, where a participant in a recognised system of the Central bank system is wound up or placed under receivership in terms of the Companies Act or any other relevant written law, any provision contained in the rules of the system or, in clearance and settlement agreement to which the participant is a party shall be binding upon the liquidator, receiver, judicial manager or administrator or other similar official, as the case may be, appointed in respect of the participant, in respect of any payment or settlement obligation which (a) was determined in accordance with the rules of the applicable system or, any clearance and settlement agreement or clearance and settlement to which the participant is a party, before the commencement of the winding up of the participant or the participant was placed under receivership, as the case may be; and (b) was either (i) to be discharged or transferred on or after the commencement of the winding up of the participant or the participant being placed under receivership; or (ii) was overdue for settlement on the commencement of the winding up of the participant or the participant being placed under receivership.”

⁵¹⁷ Act 78 of 1998 (As Amended).

⁵¹⁸ Act 4 of 2006.

⁵¹⁹ Act 1 of 2007.

or transfer which became final and irrevocable in terms of section eleven before the copy of the relevant order was lodged with the Reserve Bank in terms of section thirteen.” The reference to these two laws only limits the scope of the provision. It is therefore suggested that specific laws are not named by rather that a broader provision such as “no law, regulation, rule or practice on the setting aside of contracts and transactions” is considered.

5.7.3 Interoperable Systems

Article 3(4) of the Settlement Finality Directive (As Amended) provides that, “In the case of interoperable systems, each system determines in its own rules the moment of entry into its system, in such a way as to ensure, to the extent possible, that the rules of all interoperable systems concerned are coordinated in this regard. Unless expressly provided for by the rules of all the systems that are party to the interoperable systems, one system's rules on the moment of entry shall not be affected by any rules of the other systems with which it is interoperable.”⁵²⁰

None of the National Payment System Acts or Bills in force or being considered by SADC Member States contains any reference to, or provisions covering interoperable systems. The Mauritian legal and regulatory framework (in general) nor the specific rules and T&C's applicable to the ACH and RTGS systems also do not contain any reference to, or provisions covering interoperable systems.

5.8 Provisions Concerning Insolvency

5.8.1 The Moment of Opening of Insolvency Proceedings

Article 6(1) of the Settlement Finality Directive (As Amended) provides that, “For the purpose of this Directive, the moment of opening of insolvency proceedings shall be the moment when the relevant judicial or administrative authority handed down its decision.”

As represented in Table 42 below, most SADC countries, including Namibia, do not define the “moment of opening of insolvency proceedings” in their National Payment System Act. Other than Malawi, the only country to do so adequately is Zambia. Section 23(2) of the Zambian National Payment Systems Act, 2007⁵²¹ reads, “Notwithstanding any other law, a winding-up order shall take effect from the minute in the hour and date that it is made against the participant concerned and such order shall not affect any finality of settlement at the end of the settlement cycle.”

⁵²⁰ Article 4 reads, “Member States may provide that the opening of insolvency proceedings against a participant or a system operator of an interoperable system shall not prevent funds or securities available on the settlement account of that participant from being used to fulfil that participant's obligations in the system or in an interoperable system on the business day of the opening of the insolvency proceedings. Member States may also provide that such a participant's credit facility connected to the system be used against available, existing collateral security to fulfil that participant's obligations in the system or in an interoperable system.”

⁵²¹ Act 1 of 2007.

Table 42: Number of Countries Defining the Moment of Opening of Insolvency Proceedings

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SZ	TZ	ZM	ZW
The moment of opening of insolvency proceedings is defined in the National Payment System Act	x	x	x	x	●	x	x	x	x	x	x	x	✓	x

Malawi has adopted a detailed and practical solution to determining the moment of opening of insolvency proceedings. This moment is dependent upon the manner in which the insolvency is initiated and the initiating party.

In the case where a participant is wound-up on application by a person other than the Reserve Bank, the winding-up order must record the minute, the hour and the day that such order is made, shall be lodged with the Reserve bank on the same business day and no later than the start of the next business day and served on any other settlement agent to be notified. The Reserve Bank is required to immediately notify all relevant domestic and foreign system operators of the winding-up proceedings.⁵²² This approach is comparable to the approach set out in Article 6(1) of the Settlement Finality Directive (As Amended)."

Section 23 of the Malawian National Payment Systems Bill, 2014 requires that in the situation where a system participant is wound-up , on application by the Registrar under the Banking Act, 2009, or the Financial Services Act, 2010, the winding up must state the minute, the hour and the date on which the order is made and the Reserve Bank is required, on the same business day and in any case, no later than the start of the next business day to: (a) serve the order on the settlement system participant concerned; (b) notify other settlement system participants or agents required to be notified; and (c) notify all relevant domestic or foreign system operators.

Section 24 of the Malawian Payment System Bill, 2014 covers the situation where a participant is voluntarily wound up. In this case, subject to the provisions of the Banking Act, 2009, the Financial Services Act, 2010 or the Companies Act, 2013 the system participant that is voluntarily wound up is required to inform all other system participants of the winding-up resolution within twenty four (24) hours of the winding up resolution taking effect. It is important to notes that section 24 makes it clear that the resolution, demand or other step to wind-up a settlement system participant or operator has no effect unless approved by the Reserve Bank. As per section 24(2), the Reserve Bank is required to notify relevant domestic and foreign system operators about the voluntary winding up of a settlement system participant on the same day and in any case, no later than the start of the next business day of the winding up resolution taking effect.

The approach taken by Malawi is detailed and thorough and should be considered by other SADC Member States. Despite derogating from Article 6(1) of the Settlement Finality Directive (As Amended) which is simple and concise, the Malawian approach is recommended as it takes cognoscente of the differences in procedure, depending upon the nature of the party instituting the insolvency proceedings.⁵²³

⁵²² Section 22 National Payment Systems Bill, 2014.

⁵²³ As per section 25, "Notwithstanding the provisions of the Banking Act, 2009, the Financial Services Act, 2010, the Companies Act, 2013, the Bankruptcy Act, and any other written laws of Malawi, where a settlement system participant is wound up, the relevant winding-up order or resolution shall not affect any settlement that has become final and irrevocable in this part prior to – (a) the lodging of a copy of the order with the Reserve Bank under Section 22; (b) the

5.8.2 Notification of the Decision to the Central Bank

Article 6(2) of the Settlement Finality Directive (As Amended) requires that, when a decision has been taken in accordance with paragraph 6(1), the relevant judicial or administrative authority shall immediately notify that decision to the appropriate authority chosen by its Member State.”

The Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems does not contain a provision such as this.

Section 12 of Botswana’s National Clearance and Settlement Systems Act, 2003⁵²⁴ requires that, “where a participant in a recognised system is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act, the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued shall lodge a copy of the order with the Central Bank.” While they may look similar, section 12 of the National Clearance and Settlement Systems Act, 2003 is substantially different to Article 6(2) of the Settlement Finality Directive. In the case of the Settlement Finality Directive, the relevant judicial or administrative authority is required to notify the appropriate authority (the Central Bank) whereas in the case of Botswana’s National Clearance and Settlement Systems Act, 2003 is it “the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued”. It is recommended that the person responsible for notifying the Central Bank of the decision to commence insolvency proceedings should be the relevant judicial or administrative authority that handed down the decision to do so and not, as is the case in Botswana, the person at whose insistence the winding-up or placing under receivership is being carried out.

This requirement is contained in Article 9 of the DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 that reads, “when an insolvency proceeding is opened against an operator, the Registrar informs immediately the Central Bank. When the Central bank decides itself to open an insolvency proceedings against a participant by authorising the voluntary or forced liquidation, it mentions in its decision the exact moment when the proceedings opens.”

In terms of section 18(1) of Lesotho’s National payment System Bill, 2013 a copy of an application for insolvency must be served on the Governor by the Applicant. This provision should be reworded as it should be a copy of the decision or notification of such decision made by the relevant judicial or administrative authority that is delivered (not served) to the Governor. Such notification of the decision to open insolvency proceedings should be made by the relevant judicial or administrative authority and not by the “applicant” as is the requirement in Lesotho’s Bill. In terms of section 18(2), the Governor is required to ensure that a copy of the insolvency process is served as soon as reasonably possible to the domestic systems and operators, and if required under international cooperation arrangements with competent foreign authorities to foreign systems or operators. One again, the choice of the word “served” is inappropriate as this has an entirely different implication to simply being notified of a decision to commence insolvency proceedings.

This requirement as set out in section 22 of the Malawian Payment Systems Bill, 2014 requires that a copy of the winding-up [order] when it is made must be lodged with the Reserve Bank. Section 22 does not however state whether it is the responsibility of the applicant or the relevant judicial or administrative authority to deliver a copy of the order to the Central Bank. It is recommended that this point be clarified.

Reserve Bank informing the settlement system operator of the winding-up order under Section 22; or (c) the winding up resolution taking effect as provided under Section 23.”

⁵²⁴ Act 5 of 200

No provision such as this is found in the Mauritian law or regulation.

The Mozambican Law 02/08 of 27 February does not contain a provision such as this.

Section 4(5)(a) of the Namibian Payment System Management Act, 2003 (As Amended)⁵²⁵ requires that “when a system participant is wound up - (a) the Registrar of the High Court must lodge with the Bank a copy of the application for winding-up, if it was made, and the winding-up order within 14 days of issuance of the order.” Section 4(5)(a) of the Namibian Payment System Management Act, 2003 (As Amended) is on a par with Article 6(2) of the Settlement Finality Directive (As Amended).

In the Seychelles, as per section 13 of the National Clearance and Settlement Systems Act, 2010⁵²⁶, where a participant in a recognised system or a Central bank system is being wound up or placed under receivership in terms of the Companies Act or any other relevant law, the person at whose insistence the winding-up or placing under receivership is being carried out is required to *not less than seven days before the commencement of the winding-up of the participant or placing the participant under receivership and not more than seven days after the commencement of winding up of the participant or the participant has been placed under receivership*, send to the Central Bank, in each instance, a notice to this effect containing the prescribed particulars.

If Article 6(2) of the Settlement Finality Directive (As Amended) and section 13 of the Seychelles National Clearance and Settlement Systems Act, 2010 are compared, a number of problems with the provision in the Seychelles Act are identified. Firstly, it is recommended that the person responsible for notifying the Central Bank of the decision to commence insolvency proceedings should be the relevant judicial or administrative authority that handed down the decision to do so and not, as is the case in the Seychelles, the person at whose insistence the winding-up or placing under receivership is being carried out. Secondly, notification to the Central bank should take place immediately after the relevant judicial or administrative authority handed down its decision and not within the 14-day window as provided for in the Seychelles National Clearance and Settlement Systems Act, 2010.

In terms of section 8(4) of the South African National Payments System Act, 1998 (As Amended)⁵²⁷, “when an application for the winding-up of a clearing system participant or Reserve Bank settlement system participant is made, a copy of (a) the application for winding-up, when it is presented to the court; and (b) any subsequent winding-up order, when it is granted, must be lodged with the Reserve Bank as soon as practicable.” This provision is unclear as to whose responsibility it is to lodge the copy of the winding-up order with the Reserve Bank and should be clarified.

Section 12 of Swaziland’s National Clearing and Settlement Systems Act, 2011⁵²⁸ requires that, “where a participant in a recognised system is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act, 2009, the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued shall lodge a copy of the order with the Central Bank.” As is the case in Botswana, while section 12 of Swaziland’s National Clearing and Settlement Systems Act, 2011 may look similar to Article 6(2) of the *Settlement Finality Directive* these two provisions are substantially different. In the in the case of the Settlement Finality Directive, the relevant judicial or administrative authority is required to notify the appropriate authority

⁵²⁵ Act 18 of 2003 (As Amended).

⁵²⁶ Act 12 of 2010.

⁵²⁷ Act 78 of 1998 (As Amended).

⁵²⁸ Act 17 of 2011.

(the Central Bank) whereas in the case of Swaziland's National Clearing and Settlement Systems Act, 2011 it is "the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued". It is recommended that the person responsible for notifying the Central Bank of the decision to commence insolvency proceedings should be the relevant judicial or administrative authority that handed down the decision to do so and not, as is the case in Swaziland, the person at whose insistence the winding-up or placing under receivership is being carried out.

A notifiable event, in respect of a Participant is defined in the Tanzania Inter-Bank Settlement System Rules and Regulations as,

- "(a) Its making a general assignment for the benefit of, or entering into a reorganisation, arrangement or composition with, its creditors; or
- (b) Its admitting in writing its inability to pay its debts as they become due from its own money; or
- (c) Its seeking, consenting to or acquiescing in the appointment of any trustee, administrator, receiver or liquidator or analogous officer of it or any material part of its property; or
- (d) The presentation or filing of an application in respect of it:
 - (i) In any court or before any agency alleging or for its bankruptcy, winding up or liquidation (or any analogous proceeding) unless it can be demonstrated by the Participant to be vexatious or that it is otherwise unlikely to result in the liquidation of the Participant, in either case within a period of time to be specified by the Bank;
 - (ii) Seeking any reorganisation, arrangement, composition, readjustment, administration, liquidation, dissolution or similar relief, under any present or future statute, law or regulation, such application (except in the case of an application for liquidation or any analogous proceeding) not having been stayed or dismissed within 30 days of its filing; or
 - (iii) The appointment of a receiver, administrator, liquidator or trustee or analogous officer of it over all or any material part of its property;
- (e) The appointment of a Receiver/Manager under the Banking and Financial Institutions Act, 1991;
- (f) The occurrence of any event having a substantially similar effect to any of the events specified in (a) to (f) above under the law of any applicable jurisdiction.
- (g) A system failure that renders the Participant unable to send its normal level of payment message through the TISS;
- (h) If the Participant has good reason to doubt its authority or ability to continue to make payments or send payment messages through TISS."

In terms of Rule 19, participants must immediately upon the occurrence, or threatened occurrence, of a Notifiable Event notify the Bank of Tanzania, ensure that no further Payment Instructions are submitted to the TISS and inform the Bank of Tanzania of the steps (if any) it is taking to ensure that it continues to have the authority and ability to issue Payment Instructions. If compared against Article 6(2) of the *Settlement Finality Directive (As Amended)* this rule is deficient in a number of respects. Firstly, it does not define the moment of the opening of insolvency proceedings and secondly, it places the onus on the participant to inform the Bank of Tanzania and not on the relevant judicial or administrative authority that handed down the decision to inform the Bank of Tanzania.

This requirement is covered in section 23(1) of the *Zambian National Payment Systems Act, 2007*⁵²⁹ which reads, "notwithstanding any other law, where a participant is wound-up by a court of competent jurisdiction a copy of the winding-up order, which shall record the date and the minute in the hour that the order was passed, shall be lodged with the Bank of Zambia and served on any other settlement agent required to be notified."

⁵²⁹ Act 1 of 2007.

Section 13 of Zimbabwe's National Payment Systems Act [Chapter 24:23] requires that, "where a participant in a recognised payment system is wound up or placed under judicial management or provisional judicial management in terms of the Companies Act [Chapter 24:03], the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued shall lodge a copy of the order with the Reserve Bank." Once again, as is the case in Botswana and, while section 13 of Zimbabwe's National Payment Systems Act [Chapter 24:23] may look similar to Article of the Settlement Finality Directive these two provisions are substantially different. In the case of the Settlement Finality Directive, the relevant judicial or administrative authority is required to notify the appropriate authority (the Reserve Bank) whereas in the case of Zimbabwe's National Payment Systems Act [Chapter 24:23] it is "the person at whose instance the winding-up order or the order placing the participant under judicial management or provisional management, as the case may be, was issued". It is recommended that the person responsible for notifying the Reserve Bank of the decision to commence insolvency proceedings should be the relevant judicial or administrative authority that handed down the decision to do so and not, as is the case in Zimbabwe, the person at whose insistence the winding-up or placing under receivership is being carried out.

5.8.3 Notification of the Decision to Other Member States

Article 6(3) of the Settlement Finality Directive (As Amended) however introduces the obligations of EU Member States with respect to their obligations to inform other Member States of an insolvency decision and also to inform the European Systemic Risk Board and the European Supervisory Authority (European Securities and Markets Authority). Article 6(3) reads, "The Member State referred to in paragraph 2 shall immediately notify the European Systemic Risk Board, other Member States and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter 'ESMA'), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council." Most of the National Payment System Acts that are in force in SADC Member States are applicable to the domestic National Payment System only.

Most National Payment System Acts applicable in SADC Member States do not contain a provision of this sort. The DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 is however one of the only National Payment System Acts that requires the Central Bank to immediately inform domestic system operators as well as **foreign systems and their operators where cooperation agreements provide for this** of the opening of insolvency proceedings. It is recommended however that the BCC should inform other Central Banks (regulators) of the commencement of insolvency proceedings, rather than "foreign systems and their operators."

Lesotho's National Payment Systems Bill, 2013 requires the Governor, upon receipt of notification of insolvency proceedings initiated against a foreign system, operator or participant from a foreign competent authority under an international cooperation arrangement to, as soon as is reasonably possible, notify domestic systems, operators and participants of the initiation of insolvency proceedings.

In the light of the introduction of SIRESS, it is highly recommended that SADC Member States consider what the appropriate mechanism will be for informing other Member States of an insolvency decision and that such a mechanism is harmonised. It will also be important to consider to which "supranational" structure such a decision must be communicated.

5.8.4 No Retroactive Effects

Article 7 of the Settlement Finality Directive (As Amended) requires that, “insolvency proceedings shall not have retroactive effects on the rights and obligations of a participant arising from, or in connection with, its participation in a system before the moment of opening of such proceedings as defined in Article 6(1). This shall apply, inter alia, as regards the rights and obligations of a participant in an interoperable system, or of a system operator of an interoperable system which is not a participant.”

This requirement is inferred in Article 20 of the Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems but is generally considered to be insufficient.

Section 13 of Botswana’s National Clearance and Settlement Systems Act, 2003⁵³⁰ reads, “notwithstanding anything to the contrary in the Insolvency Act or the Companies Act, the winding up of a participant in a recognised system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section 10 before the copy of the relevant order was lodged with the Central Bank in terms of section 14.” While the provision in Botswana’s National Clearance and Settlement Systems Act, 2003 has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgement of a copy of the order with the Bank. As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgement of a copy of the order with the Bank.

The DRC’s Draft Law on the Provisions Applicable to the National Payment System, 2013 is one of the few Acts that actually uses the words “retroactive effects.” In this regard, Article 6 reads, “the insolvency proceedings opened for a participant has no retroactive effect on the rights and obligations of a participant from his participation in a system, or in relation with the said participation, before the opening of his insolvency proceedings.”

Section 25 of the Malawian Payment System Bill has the effect of insolvency proceedings not having retroactive effects. It is however recommended that Malawi consider referring to the “rights and obligations of a participant in an interoperable system, or of a system operator of an interoperable system which is not a participant.”

No provision such as Article 7 of the Settlement Finality Directive (As Amended) is found in the Mauritian law or regulation.

This requirement is inferred in Article 16 of Mozambican Law 02/08 of 27 February but is generally considered to be insufficient.

Section 4(5)(b) of the Namibian Payment System Management Act, 2003⁵³¹ reads, “despite sections 341(2) and 348 of the Companies Act, the winding-up order does not affect any settlement that has become final and irrevocable prior to the lodgement of the copy of that order with the Bank in terms of paragraph (a).” While the Namibian provision has the effect of insolvency proceedings not having retroactive effects, the words

⁵³⁰ Act 5 of 2003.

⁵³¹ Act 18 of 2003 (As Amended).

“retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgement of a copy of the order with the Bank. As such, it may be advisable to reword this provision and choose the moment of opening of insolvency proceedings as the cut off time rather than the lodgement of a copy of the order with the Bank.

The provisions found in the Seychelles National Clearance and Settlement Systems, 2010⁵³² have the effect of insolvency proceedings not having retroactive effects, however, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgment of a copy of the order with the Bank (The Seychelles Act allows for seven days after the commencement of winding-up of a participant). As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgment of a copy of the order with the Bank.

While the South African National Payments System Act, 1998 (As Amended)⁵³³ does not specifically refer to “insolvency proceedings not having retroactive effects”, this is inferred.

Section 13 of Swaziland’s National Clearing and Settlement Systems Act, 2011⁵³⁴ “notwithstanding anything to the contrary in the Insolvency Act, 1955 or the Companies Act, 2009, the winding up of a participant in a recognised or Central Bank system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section 10 before the copy of the relevant order was lodged with the Central Bank in terms of section 12.” While the provision found in Swaziland’s National Clearing and Settlement Systems Act, 2011 has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgement of a copy of the order with the Bank. As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgement of a copy of the order with the Bank.

No provision such as Article 7 of the Settlement Finality Directive (As Amended) is found in the Tanzanian law or regulation.

This requirement is covered by section 20(2) of the Zambian National Payment Systems Act, 2007⁵³⁵, although the words “retroactive effects” are not used.

In terms of section 14 of Zimbabwe’s National Payment Systems Act [Chapter 24:23], “notwithstanding anything to the contrary in the Insolvency Act [Chapter 6:04] or the Companies Act [Chapter 24:03], the winding up of a participant in a recognised payment system, or the placing of such a participant under judicial management or provisional judicial management, shall not affect the finality or irrevocability of any payment or transfer which became final and irrevocable in terms of section eleven before the copy of the relevant order was lodged with the Reserve Bank in terms of section thirteen.”

⁵³² Act 12 of 2010.

⁵³³ Act 78 of 1998 (As Amended).

⁵³⁴ Act 17 of 2011.

⁵³⁵ Act 1 of 2007.

While the Zimbabwean provision has the effect of insolvency proceedings not having retroactive effects, the words “retroactive effects” are not used and once again, the fact that the “moment of opening of insolvency proceedings” is not defined, may be problematic. There may also be a considerable time delay between the moment of opening of insolvency proceedings and the lodgement of a copy of the order with the Bank. As such, it may be advisable to reword this provision and chose the moment of opening of insolvency proceedings as the cut off time rather than the lodgement of a copy of the order with the Bank.

5.9 Collateral Security

“The reduction of credit and systemic risk requires, in addition to the finality of settlement, the enforceability of collateral. This implies that collateral should be insulated from the effects of the insolvency legislation applicable to an insolvent collateral provider (i.e. the collateral taker should be sure that collateral received cannot be challenged in an insolvency procedure).”⁵³⁶

The EU approach to the insulation of collateral security is set out in Article 9 of the Settlement Finality Directive (As Amended). Article 9(1) reads, “the rights of a system operator or of a participant to collateral security provided to them in connection with a system or any interoperable system, and the rights of central banks of the Member States or the European Central Bank to collateral security provided to them, shall not be affected by insolvency proceedings against:

- (a) the participant (in the system concerned or in an interoperable system);
- (b) the system operator of an interoperable system which is not a participant;
- (c) a counterparty to central banks of the Member States or the European Central Bank; or
- (d) any third party which provided the collateral security.

Such collateral security may be realised for the satisfaction of those rights.”⁵³⁷

The provision on collateral security in the Angolan Law nº 5/05 Dated July 29 Law of Angolan Payment Systems are found in various articles scattered throughout the Act. Article 15(3) that refers to “the formation of a special heritage comprising assets and rights” is unclear as to the intent of the Article. Article 20 (1) that requires that “the product from the execution of guarantees made to the subsystem or clearing house by the participant, as well as the securities, subject to the negotiation of guarantees, shall be intended for the settlement of obligations undertaken by the participants in the said subsystems or clearing houses” is also unclear and does not provide the clarity provided by a provision such as Article 9 of the Settlement Finality Directive (As Amended). We maintain that the Angolan provisions do not adequately provide for the insulation of collateral security from the effects of insolvency in the domestic context. Law nº 05/05 Dated July 29 also does not make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

⁵³⁶ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 147.

⁵³⁷ Article 9(2) reads, “where securities including rights in securities are provided as collateral security to participants, system operators or to central banks of the Member States or the European Central Bank as described in paragraph 1, and their right or that of any nominee, agent or third party acting on their behalf with respect to the securities is legally recorded on a register, account or centralised deposit system located in a Member State, the determination of the rights of such entities as holders of collateral security in relation to those securities shall be governed by the law of that Member State.”

Botswana's National Clearance and Settlement Systems Act, 2003⁵³⁸ does not contain a provision on the insulation of the rights of holders of collateral security from the effects of insolvency of the Provider. This is highlighted as a substantial gap in the Law. The National Clearance and Settlement Systems Act, 2003 also makes no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The provision on collateral security in the DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 is found in several articles of the Draft Law. These are Article 8, Article 12, Article 13, and Article 15. While it is arguable that these provisions are adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context, they make no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The provisions on collateral security in the Lesotho's National Payment Systems Bill, 2013 are found in Part IV of Act. Section 20 sets out the scope of application,⁵³⁹ section 21 the validity and enforceability of financial collateral arrangements,⁵⁴⁰ section 22 the validity and enforceability of close-out netting provisions,⁵⁴¹ section 23 the protection of substitution and topping-up collateral,⁵⁴² section 24 the realisation of pledged financial collateral⁵⁴³ and section 25 the prevalence of rights of a collateral taker.⁵⁴⁴ These provisions read collectively are one of the most comprehensive sets of provisions on collateral found in the National Payment System Acts/Bills applicable in SADC Member States.

These provisions found in Lesotho's National Payment Systems Bill, 2013 are adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context. It must however be noted that until the Bill is promulgated and becomes a legally enforceable Act, the provisions of the Insolvency Proclamation No. 51 of 1957 prevail and any collateral provided could, legally be affected by insolvency proceedings against a participant. This same concern applies to the DRC and Malawi as well.

⁵³⁸ Act 5 of 2003.

⁵³⁹ Section 20 reads, "for purposes of this Part, financial collateral arrangements include present, future, actual, contingent or prospective obligations owed to a collateral taker, or his or her principal, by a collateral provider or by another person."

⁵⁴⁰ Section 21 reads, "A financial collateral arrangement under this Act is valid and enforceable against third parties, including a liquidator, and takes effect in accordance with its terms:

Provided that: (a) it is in writing; (b) the possession of the financial instrument or precious metal subject to the financial collateral arrangement is transferred to the collateral taker; (c) the possession of the cash subject to the financial collateral arrangement is transferred to the collateral taker."

⁵⁴¹ Section 22 reads, "close-out netting provisions shall take effect upon the Governor notifying the operators of the system of the event of institution of insolvency proceedings."

⁵⁴² Section 23 reads, "(1) A financial collateral arrangement may contain: (a) an obligation to provide financial collateral or additional financial collateral in order to take account of changes in the value of the financial collateral or in the amount of the guaranteed obligations; (b) a right to withdraw financial collateral on providing, by way of substitution or exchange, financial collateral of substantially the same value. (2) Execution of a financial collateral under subsection (1) is valid and enforceable against third parties, including a liquidator."

⁵⁴³ Section 24 reads, "on the occurrence of an enforcement event and notwithstanding the institution of insolvency proceedings in respect of the collateral taker or collateral giver, the collateral taker may realise, in the following manner, a financial collateral provided under this Act, and subject to the terms agreed: (a) by sale and setting off the value of the financial instrument or precious metal against the guaranteed obligations; or (b) by sale and setting off the value of the financial instrument or precious metal by applying its value in the discharge of the guaranteed obligations; (c) cash by setting off the amount against or applying it in discharge of the guaranteed obligations."

⁵⁴⁴ Section 25 reads, "the rights of a collateral taker to a financial collateral arrangement shall prevail over the rights of any other creditor."

Lesotho's National Payment Systems Bill, 2013 does not make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The provision on collateral security in the Malawian Bill, 2014 is found in sections 30 and 31 of the Bill. Specifically, section 31 reads,

"Notwithstanding the provisions of any other written law, any asset of a clearing or settlement system participant which the clearing or settlement system participant, prior to the issue of its winding-up order, provided to -

- (a) the Reserve Bank as security for a loan or otherwise as security in respect of its settlement obligations; or
- (b) a clearing or settlement system in form of a written agreement as security in respect of its payment obligations,

May be utilised by the Reserve Bank or the clearing or settlement system operator to the extent required for the discharge of such settlement obligations or payment obligations as the case may be."

This provision is adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context. It does not, however, make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The Mauritian laws and regulations do not contain provisions on the insulation of collateral security from the effects of insolvency in the domestic context. Laws and regulations also make no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

Two provisions on collateral security in the Mozambican Law 02/08 of 27 February are found in Articles 14 and 15 of the Act. Article 14(1) reads, "any securities considered appropriate by the *Banco de Moçambique* may be used as guarantee for the settlement of obligations by the payments subsystems, taking into account the goals of monetary policy, namely: (a) Treasury Bonds; (b) Treasury Bills; (c) Monetary Authority Bills." Article 14(2) states that any guarantees provided for the purposes mentioned in the clause above shall be immune from seizure until the obligations to which they are related have been settled. Article 15 covers the execution of guarantees and the priority of certain obligations in the circumstance of non-performance of a participant in a payment subsystem. While it can be argued that Article 14 is adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context, Article 14 makes no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The provision on collateral security in the Namibian Payment System Management Act, 2003 (As Amended)⁵⁴⁵ is found in section 9 of the Act that reads, "despite anything to the contrary in the Insolvency Act, any asset of a system participant which the system participant, prior to the issue of its winding-up order, has provided -

⁵⁴⁵ Act 18 of 2003 (As Amended).

- (a) to the Bank as security for a loan in respect of its settlement obligation, may be utilised by the Bank to the extent required for the discharge of that settlement obligation; or
- (b) in terms of a written agreement with a service provider, to the service provider as security in respect of its payment obligation, may be utilised by the service provider to the extent required for the discharge of that payment obligation.”

This provision is adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context. It does not, however, make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The Seychelles National Clearance and Settlement Systems Act, 2010⁵⁴⁶ does not contain a provision on the insulation of the rights of holders of collateral security from the effects of insolvency of the Provider. This is highlighted as a substantial gap in the Law. The National Clearance and Settlement Systems Act, 2010 also makes no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

The provision on collateral security in the South African National Payments System Act 78 of 1998 (As Amended) is found in section 9 of the Act that reads, “despite anything to the contrary in any law relating to insolvency, any asset of a settlement system participant which was provided prior to the issue of any order for that settlement system participant’s winding-up by that participant to the Reserve Bank of the designated settlement system operator as security for a loan in respect of its settlement obligations, may be utilised by the Reserve Bank or the designated system operator, as the case may be, to the extent required for the discharge of those settlement obligations of the settlement system participant.”

This provision is adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context. It does not, however, make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

Swaziland’s National Clearing and Settlement Systems Act, 2011⁵⁴⁷ does not contain a provision on the insulation of the rights of holders of collateral security from the effects of insolvency of the Provider. This is highlighted as a substantial gap in the Law. The Act also makes no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

Rule 39 of the Tanzania Inter-Bank Settlement System Rules and Regulations reads as follows:

“(1) The Bank may, at its discretion, extend Intraday Liquidity Facility (ILF) to Participants to assist them meet their intraday liquidity requirements under TISS. The ILF must be fully secured by eligible collateral securities, in such manner as prescribed by the Bank.

(2) The Bank shall establish the amount and collateral arrangements for the ILF with each Participant.”

This is the only reference to collateral security and the TISS Rules and Regulations contain no provisions on the insulation of collateral security from the effects of insolvency in the domestic context. The Rules and Regulations also do not, make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

⁵⁴⁶ Act 12 of 2010.

⁵⁴⁷ Act 17 of 2011.

The provision on collateral security in the Zambia is found in section 26 of the Act that reads, “Notwithstanding anything to the contrary contained in the Banking and Financial Services Act, Companies Act, Bankruptcy Act or any other law, any asset of a participant provided as collateral for settlement obligations prior to the issue of any order for that participant’s winding-up may be utilised by the Bank of Zambia (a) to the extent required for the discharge of such settlement obligations; (b) as collateral for the discharge of its settlement obligations in terms of a written agreement with any clearing house; or in accordance with the Banking and Financial Services Act.” This provision is adequate as far as the insulation of collateral security from the effects of insolvency in the domestic context. It does not, however, make any reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

Zimbabwe’s National Payment Systems Act [Chapter 24:23] does not contain a provision on the insulation of the rights of holders of collateral security from the effects of insolvency of the Provider. This is highlighted as a substantial gap in the Law. The Act also makes no reference to collateral security that may be provided in connection with an interoperable system, nor to the rights of central banks of Member States.

All fourteen SADC Member States will need to consider amending their domestic legislation to cater for participation in SIRESS. An example of how Article 9(1) of the Settlement Finality Directive (As Amended) was transposed by Ireland into their domestic regulation is provided below. The Irish Statutory Instrument S.I. No. 539/1998 - European Communities (Finality of Settlement in Payment and Securities Settlement Systems) Regulations, 1998 transposes the mandatory provisions of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems into domestic Irish law. (See [Annexure O](#) of this report). Regulation 7(2) of the Irish Statutory Instrument reads, “where securities (including rights in securities) are provided as collateral security to members or to central banks of the Member States or to the European Central Bank, and their right (or that of any nominee, agent or third party acting on their behalf) with respect to the securities is legally recorded on a register, account or centralised deposit system located in a Member State of the European Union, the determination of the rights of such entities as holders of the collateral security in relation to those securities shall be governed by the law of that Member State.”

5.10 Prohibition against Payment Intermediation

As indicated in Table 43 below, most National Payment System Acts / Bills contain a prohibition against payment intermediation. The provisions set out in the Tanzanian National Payment System Bill are unknown at this time. Section 7 of the Namibian Payment System Management Act, 2003 (As Amended)⁵⁴⁸ is considered to be a well drafted provision and could serve as a benchmark for the proposed harmonised Model Law.

⁵⁴⁸ Act 18 of 2003 (As Amended).

Table 43: Provision on the Prohibition of Payment Intermediation found in the Domestic National Payment System Act

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SZ	TZ	ZM	ZW	SADC
PAYMENT INTERMEDIATION															
Prohibition against payment intermediation	✓	✓	✗	●	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	11
Prohibition cannot be construed as prohibiting the acceptance of money or payment instructions by a holding company from its subsidiary or by an agent of a holding company	✗	✓	✗	✗	●	✗	✗	✓	✓	✗	✓	✗	✓	✓	7
Minister may, after consultation with the Central Bank exempt any person from the prohibition if satisfied that such an exemption is in the public interest	✗	✓	✗	✗	●	✗	✗	✓	✓	✗	✓	✗	✓	✓	7

5.11 Conflict of Laws

Kokkola notes that, “where a system provides cross-border (or multi-currency) services, has cross-border linkages or has foreign (or remote) participants, the rules governing that system should clearly indicate the national legislation applicable to each aspect of the functioning of the system. The operators of cross-border systems must address the issue of conflicts of law where there are differences between the substantive legislation applicable in the various jurisdictions with a potential interest in the system. Each individual jurisdiction has rules on conflicts of law that specify the criteria that determine the national legislation applicable to such a system. System operators and participants should be aware of the issues surrounding conflicts of law when structuring the rules of a system and choosing the national legislation that governs that system. System operators and participants should also be aware of any constraints on their ability to choose the legislation that will govern the system in question.”⁵⁴⁹

Further, “it will not be possible for system operators and participants to circumvent the fundamental public policy of their jurisdiction by means of a contractual choice. Such ‘public law’ provisions are usually found in legislation concerning insolvency and the equal treatment of creditors. Subject to such constraints, the legal framework should support appropriate contractual choices as regards the legislation to be applied in the context of domestic and cross-border operations. In many cases, the legislation chosen will be that of the country where the system is located.”⁵⁵⁰

The issue of conflict of law was solved in the EU through the Settlement Finality Directive and the Financial Collateral Directive. Both these supranational legal instruments seek to achieve the desired legal certainty for

⁵⁴⁹ Kokkola *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* 149.

⁵⁵⁰ 149.

systems' cross-border operations. Article 9 of each contains rules minimising conflicts of law. These have made a significant contribution to the free cross-border movement of payments and collateral within the EU. The Directives both adopt the "place of the relevant intermediary approach" (PRIMA).

Explaining how this principle works, Kokkola states, "Article 9 of the Settlement Finality Directive specifies that where securities (including rights in securities) are given as collateral to a clearing or settlement system or the central bank of an EU Member State and the right of that system or central bank (or that of any nominee, agent or third party acting on its behalf) in respect of the securities is legally recorded in a register, account or centralised deposit system located in Member State X, the determination of the rights of such entities as holders of collateral security in relation to those securities is governed by the law of Member State X. However, that provision applies only to systems and central banks. Consequently, securities provided under other collateral arrangements in the EU are governed by a similar principle (based on Article 9 of the Financial Collateral Directive) concerning the location of the relevant account."⁵⁵¹

Most National Payment System Acts, Bills of Draft Bills do not contain any conflict of law provisions. In light of each SADC Member States current or future participation in SIRESS, this is highlighted as a gap that needs to be rectified as soon as possible.

A good example of such a provision is however found in Article 11 of the DRC's Draft Law on the Provisions Applicable to National Payment Systems, 2013. This Article which covers the insolvency of a foreign participant in a payment system governed by the DRC's Act or the insolvency of a domestic (DRC) participant in a foreign payment system reads, "should an insolvency proceeding open against a foreign participant in a payment system governed by this Act, the rights and obligations inherent to the participation of this foreign participant, are entirely and exclusively governed by the Congolese legislation. Should an insolvency proceeding open against a domestic participant in a foreign payment system, the rights and obligations inherent or linked to the participation of this participant to such a system are entirely and exclusively governed and determined by the Act governing that foreign system."⁵⁵²

5.12 Dispute Resolution

5.12.1 Domestic Arbitration

In his paper, *Arbitration as a Tool for Strengthening Cross-Border Deals: Making a Case for the Harmonisation of Arbitration Laws in the SADC Region*, Bagshaw notes that, "domestic arbitration is an alternative to Court, where parties in dispute can agree on their preferred tribunal and the detailed nature of their procedure. It involves parties who are based in the same jurisdiction doing business in that jurisdiction, and therefore they could choose the local courts, with judges all of one nationality, hearing cases only within that state, and applying the procedures and culture of that state, without any one party feeling that they were subjecting themselves to the another party's tribunal. Domestic arbitration needs, and usually offers, the ready availability of court assistance. It is obvious which courts will do this since the case only concerns parties and projects in one jurisdiction."⁵⁵³

⁵⁵¹ 150.

⁵⁵² Article 18 of the DRC's draft law reads, "the book-entry of a financial collateral is governed by the legislation of the country in which the account is held."

⁵⁵³ Bagshaw D 2013 *Arbitration as a Tool for Strengthening Cross-Border Deals: Making a Case for the Harmonisation of Arbitration Laws in the SADC Region* Lilongwe, Malawi.

As depicted in Table 44 below, most SADC Member States include a dispute settlement provision in their National Payment System Act or Bill. The notable exceptions are the DRC and Lesotho. In the absence of a National Payment System Act in Mauritius, parties to a dispute (either a dispute between the Central Bank and a Participant in MACSS or between two or more parties) are required to follow the dispute resolution mechanism set out in the Mauritius Automated Clearing and Settlement System (MACSS) T&C's.⁵⁵⁴ In Tanzania, in the absence of a legally enforceable National Payment System Act, participants in the Tanzania Inter-Bank Settlement System (TISS) are required to follow the dispute resolution mechanisms set out in the Tanzania Inter-Bank Settlement System Rules and Regulations. In terms of Rule 94, in the case of any dispute arising between the participants with regard to the construction of the Rules and Regulations or the rights, duties or obligations of the participants, including any dispute in respect of and termination of the Agreement to Participate in TISS, such dispute must be referred to arbitration by the Inter-Bank Settlement System Dispute Resolution Committee as established in section 95.⁵⁵⁵

Mauritius is the only country that does not have a National Payment System Act. All ten countries that have included dispute settlement provisions in a legally enforceable National Payment System Act or Bill, mandate conciliation, mediation and arbitration, as the alternative dispute resolution mechanism. The application of the national Arbitration Act is specifically mandated by eight SADC Member States.

It is specifically noted that none of the National Payment System Acts contain dispute settlement provisions / out of court complaint and redress procedures applicable to payment service providers and payment service users. This matter is covered in [Regulation \(EC\) No 924/2009 on Cross-Border Payments in the Community](#), and, in light of the introduction of SIRESS and the possible addition of various retail streams in the future, should be considered by SADC member States. According to Article 11 of the Regulation (EC) No 924/2009, Member States are required to establish adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and their payment service providers. Member States were required to notify the Commission of their out-of-court complaints and redress bodies by 29 April 2010.

Table 44: Domestic Dispute Resolution Provisions in National Payment System Acts / Bills

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
Domestic Dispute Resolution Mechanism															

⁵⁵⁴ The same process is set out in the PLACH Rules.

⁵⁵⁵ Rule 95 reads, "The Inter-Bank Settlement System Dispute Resolution Committee shall comprise of ten (10) members made up as follows: (i) Two members from the Bank and; (ii) Eight rotating members, appointed by participants, for purpose of continuity four new members shall be appointed each year; (2) A "Secretary" shall be appointed among the members to act in an ex-officio capacity for one year. (3) The Chairman of the Committee shall be a member from the Bank conversant with the TISS system; (4) The vice chairman shall be elect annually among the members; (5) A committee member shall cease to be a member of the Committee if the participant he/she represents ceases to be a participant of TISS. (6) The Committee meetings shall be held at least once every two months or at any time in case of an extraordinary meeting and the minutes thereof submitted to the members of the Committee. The quorum of the committee shall be five members and a representative from the Bank. (7) The decisions of the Committee shall be on the basis of a simple majority vote, with the Chairman having a casting vote."

National Payment System Act Contains a Domestic Dispute Resolution Provision	✓	✓	✗	✗	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	10
Conciliation, Mediation & Arbitration Mandated in the National Payment System Act as the Domestic Dispute Resolution Mechanism	✓	✓	✗	✗	●	✗	✓	✓	✓	✓	✓	✓ ⁵⁵⁶	✓	✓	10
Application of the National Arbitration Act is Mandated in the National Payment System Act	✗	✗	✗	✗	●	✗	✓	✓	✓	✓	✓	✗	✓	✓	8
Scope: Parties (Central Bank Settlement System Participant and Central Bank)	✓	✓	✗	✗	●	✗	✓	✓	✓	✓	✓	✓ ⁵⁵⁷	✓	✓	10
Out of court complain and redress procedure (PSPs and Users)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	0

5.12.2 International Arbitration

International arbitration, as compared to domestic arbitration is a completely different matter. International arbitration needs to accommodate as far as possible the wishes of parties from different cultures, both legal and in the wider sense. This means that they need to be able to freely select the nationality of the tribunal, the place of hearings and the extent of court interference. It is also important that foreign arbitral awards are recognised and enforced. In this regard, the *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, also known as the "New York Arbitration Convention" or the "New York Convention," is one of the key instruments in international arbitration. The New York Convention applies to the recognition and enforcement of foreign arbitral awards and the referral by a court to arbitration.

As noted on the New York Arbitration Convention website, *"the two basic actions contemplated by the New York Convention are the recognition and enforcement of foreign arbitral awards and the referral by a court to arbitration. The first action is the recognition and enforcement of foreign arbitral awards, i.e., arbitral awards made in the territory of another (Contracting) State. This field of application is defined in Article I. The general obligation for the Contracting States to recognise such awards as binding and to enforce them in accordance with their rules of procedure is laid down in Article III. A party seeking enforcement of a foreign award needs to supply to the court (a) the arbitral award and (b) the arbitration agreement (Article IV). The party against whom enforcement is sought can object to the enforcement by submitting proof of one of the grounds for refusal of enforcement which are listed in Article V(1). The court may on its own motion refuse enforcement for reasons of public policy as provided in Article V(2). If the award is subject to an action for setting aside in the country in which, or under the law of which, it is made ("the country of origin"), the foreign court before which enforcement of the award is sought may adjourn its decision on enforcement (Article VI). Finally, if a party seeking enforcement prefers to base its request for enforcement on the court's domestic law on enforcement of foreign awards or bilateral or other multilateral treaties*

⁵⁵⁶ Rule 94 Tanzania Inter-Bank Settlement System Rules and Regulations.

⁵⁵⁷ The TISS Rules and Regulations refer to a "dispute or difference between the Bank and the Participant; or two or more Participants, arising out of, or in any way connected with, these Rules and Regulations."

in force in the country where it seeks enforcement, it is allowed to do so by virtue of the so-called more-favourable-right provision of Article VII(1).

The second action contemplated by the New York Convention is the referral by a court to arbitration. Article II(3) provides that a court of a Contracting State, when seized of a matter in respect of which the parties have made an arbitration agreement, must, at the request of one of the parties, refer them to arbitration (unless the arbitration agreement is invalid). In both actions the arbitration agreement must satisfy the requirements of Article II(1) and (2) which include in particular that the agreement be in writing.”

As depicted in Table 45 below, only 9 SADC Member States are contracting parties to the Convention on the Enforcement of Foreign Arbitral Awards (the New York Convention).

Table 45: International Dispute Resolution Mechanism

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW	SADC
International Dispute Resolution Mechanism															
International Arbitration Act based on the UNCITRAL Model Law on International Commercial Arbitration	x	x	✓	x	x	✓	x	x	x	x	x	x	✓	✓	4
Country is a contracting state to the Convention on the Enforcement of Foreign Arbitral Awards (the New York Convention)	x	✓	✓	✓	x	✓	✓	x	x	✓	x	✓	✓	✓	9
Implementing Act	x	✓	✓	✓	x	✓	✓	x	x	✓	x	x	✓		7

It must be noted that Mauritius is positioning itself as the African arbitration seat of choice. It passed an *International Arbitration Act in 2008*, which it amended in 2013, and which is amongst the most arbitration-friendly worldwide. Mauritius is a party to the New York Convention. In addition, the 2013 amendments to the International Arbitration Act provide that international arbitration matters will be heard by judges from a panel of “Designated Judges”, i.e. these judges will have expertise in international arbitration. Mauritius launched an international arbitration centre, the LCIA-MIAC Arbitration Centre, in 2011. The choice of Mauritius as a viable seat of arbitration for potential disputes that may arise between SIRESS participants should not be ruled out in the future.⁵⁵⁸ Such arbitrations would be conducted under the LCIA-MIAC arbitration rules that are universally applicable and suitable for all types of disputes. The LCIA-MIAC arbitration rules offer a combination of the best features of the civil and common law systems, including:

- Maximum flexibility for parties and tribunals to agree on procedural matters;
- Speed and efficiency in the appointment of arbitrators, including expedited procedures;

⁵⁵⁸ Parties to LCIA-MIAC arbitration may be from any geographical location. Although LCIA-MIAC is based in Mauritius, the parties are free to agree the seat, or legal place, of the arbitration. Parties wishing to provide for a seat elsewhere than Mauritius should not, therefore, be deterred from adopting the LCIA-MIAC rules. If parties adopting the LCIA-MIAC rules do not specify the seat in their agreement, Article 16.1 of the rules provides for Mauritius as the default seat. If, however, one or more of the parties wishes to argue for an alternative seat, the LCIA Court will decide the issue. Hearings may be held in Mauritius even if the seat is elsewhere, or in any other location convenient to the parties and the Tribunal.

- Means of reducing delays and counteracting delaying tactics;
- Tribunals' power to decide on their own jurisdiction;
- A range of interim and conservatory measures;
- Tribunals' power to order security for claims and for costs;
- Special powers for joinder of third parties;
- Waiver of right of appeal;
- Costs computed without regard to the amount in dispute;
- Staged deposits - parties are not required to pay for the whole arbitration in advance.⁵⁵⁹

SECTION 6: ELECTRONIC DOCUMENTS, TRANSACTIONS AND SIGNATURES

As discussed in section 3.1.2 of this report, the UNCITRAL Model Law on Electronic Commerce is based on three fundamental principles, namely, 1) functional equivalence, 2) technology neutrality and 3) party autonomy. Applying these three principles, the Model Law covers the legal recognition of data messages, writing, signatures, originals, admissibility and evidentiary weight of data messages, retention of data messages, formation and validity of contracts, recognition of parties of data messages, attribution of data messages, acknowledgement of receipt and the time and place of dispatch and receipt of data messages.

Most National Payment System Acts in the region do not contain any provisions on electronic documents, transactions, data messages or signatures. Some countries⁵⁶⁰ and the Seychelles⁵⁶¹ and have included provisions on the *prima facie* admissibility of electronic and optical evidence, if compared to the provisions found in the DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 it is clear that these provisions should be updated and revised. Articles 62 to 66 of the DRC's Draft Law on the Provisions Applicable to the National Payment System, 2013 covers 1) payment orders kept in archives in electronic format constitute proof and are legally admissible, 2) writing in electronic format is accepted as proof; 3) documents in electronic format must be kept for a period of 10 years, 4) secure electronic signature linked to an electronic certificate are accepted as and carry the evidentiary weight as handwritten signatures, 5)

⁵⁵⁹ See <http://www.lcia-miac.org/arbitration/arbitration.aspx>

⁵⁶⁰ Lesotho's National Payment Systems Bill, 2014 contains two relevant provisions. Section 26 that covers the admissibility of electronic and optical evidence reads, "the existence, the content and the timing of any transfer order, its entry into a system, as well as its execution shall be admissible evidence in all cases, be it civil, commercial, criminal or administrative, against any participants or third parties in writing or in a durable medium ensuring its traceability, be it in an electronic or optical form, including the out print of such electronic or optical document." Section 27 states that the "archives of a bank may be held in the form of a durable medium ensuring their traceability, be it in an electronic or optical form, including the out print of such electronic or optical document."

⁵⁶¹ The Seychelles National Clearance and Settlement Systems Act 12 of 2010 contains two relevant provisions. These are section 22 and section 23. Section 22 reads, "the entries relating to a system or a clearance and settlement system in ledgers, day-books, cash books and other accounts of any participant, whether captured manually by handwriting or computerized shall be *prima facie* evidence of the matters, transactions and accounts therein recorded, on proof being given by affidavit in writing of one of the directors, managers, or officers of such participant or by oral evidence, that the ledgers, day books, cash books or other account books are or have been the ordinary books of such participant and that the said entries have been made in the usual and ordinary course of business, and that the books are in or come immediately from the custody or control of the participant." Section 23 reads, "notwithstanding any other written law to the contrary, photographic images such as film, microfilm, microfiche, or computer images of the original documents such as cheques or other payment instruments, securities, certificates of deposits, account ledgers, shall be admissible as *prima facie* evidence of the matters, and or transactions of the original instrument, on proof being given on written affidavit or by oral testimony."

institutions who would like to set up or operate an electronic certification system must be approved by the Central Bank. Even in the DRC, it is however recommended that in the absence of an Electronic Transactions and Communications Act that the DRC consider revising these provisions by using the UNCITRAL Model Law on Electronic Commerce (1996) as a best practice benchmark.

Mauritius, South Africa and Zambia although their National Payment System Acts do not contain provisions on electronic documents, transactions and signatures have enacted comprehensive *Electronic Transactions and Communications Acts*. The Seychelles has also enacted a similar Act. These Acts provide evidentiary proof of authentication of electronic payments using digital signatures or other instruments for electronic payment authorisation. The laws also provide for the establishment and maintenance of a register of cryptography providers and the accreditation of authentication products and services in support of advanced electronic signatures by a recognised Accreditation Authority.

6.1 Scope and Content of Relevant Provisions found in the South African Electronic Communications and Transactions Act, 2002

South Africa's Electronic Communications and Transactions Act, 2002⁵⁶² was promulgated in 2002 and is widely considered to be one of the benchmark statutes in the SADC region.⁵⁶³ The Electronic Communications and Transactions Act, 2002 contains all of the suggested provisions contained in the UNCITRAL Model Law of Electronic Commerce (1996) and the UNCITRAL Model Law on Electronic Signatures (2001). In addition, the law covers several additional topics including: consumer protection (Chapter VII); protection of personal information (Chapter VIII); protection of critical databases (Chapter IX); domain name authority and administration (Chapter X); limitation of liability of service providers (Chapter XI); cyber inspectors (chapter XII) and cybercrime (chapter XIII).

For the purpose of providing a frame of reference for other countries that may be considering enacting such a statute or making amendment to the National Payment System Act to include salient provisions, the scope and content of the provisions found in the Electronic Communications and Transactions Act, 2002, as they pertain particularly to payments related matters are set out below.

FOCUS AREA 1: LEGAL REQUIREMENTS FOR DATA MESSAGES

Legal recognition of data messages: Section 11(1) of the Electronic Communications and Transactions Act, 2002⁵⁶⁴ states clearly that, "information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message."⁵⁶⁵ Additionally, information is not without legal force and

⁵⁶² Act 25 of 2002.

⁵⁶³ See Mambi 2012 Presentation on E-Transaction and E-Commerce Assessment Report where the presenter notes that, "Generally, four countries namely Mauritius, Seychelles, South Africa and Namibia has specific laws that address key issues on e-transactions and e-commerce. The frameworks provide for comprehensive language utilised to effect policy best practice. However, the laws in Mauritius and Seychelles do not have specific provisions on consumer protection online. The Law in Seychelles do not have specific provisions admissibility of electronic evidence." The presenter notes further that, "Laws from the Republic of South Africa and Zambia can be used as best practises in the sense that all issues related to cyber security such as e-transaction, e-commerce, cybercrimes, data protection and consumer protection are all provided in one law."

⁵⁶⁴ Act 25 of 2002.

⁵⁶⁵ Data message is defined as, "data generated, sent, received or stored by electronic means and includes voice, where the voice is used in an automated transaction and a stored record."

effect merely on the grounds that it is not contained in the data message purposing to give rise to such legal force and effect, but is merely referred to in the data message (Article 11(2)).⁵⁶⁶

Writing: Section 12 states that if there is a requirement in law that a document or information must be in writing, this requirement is met if the document or information is in the form of a data message or, is accessible in a manner usable for future reference.

Signature: Section 13 covers the topic of electronic signatures. In terms of section 13(1), where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.⁵⁶⁷ However, subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form (section 13(2)).

Section 13(3) states that, "where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-

- (a) a method is used to identify the person and to indicate the person's approval of the information communicated: and
- (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated."

Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved (Section 13(4)).

In the case where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that it is in the form of a data message or, it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred (Section 13(5)).

Original: In cases where the law requires that information is to be presented or retained in its original form, this requirement is met by a data message if the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and that information is capable of being displayed or produced to the person to whom it is to be presented (Section 14(1)(a) and (b)).

Section 14(2) requires the integrity of information to be assessed by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display, in the light of the purpose for which the information was generated; and having regard to all other relevant circumstances.

⁵⁶⁶ In terms of section 11(3) of the of the Electronic Communications and Transactions Act, 2002 , information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is (a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and (b) accessible in a form which it may be reads, stored and retrieved by the other party, whether electronically or as a computer printout as, long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

⁵⁶⁷ An advanced electronic signature is defined as, "an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37."

Admissibility and evidential weight of data messages: Section 15(1) prohibits the application of the rules of evidence in any legal proceedings so as to deny the admissibility of the electronic message in evidence on the mere grounds that it is constituted by a data message; or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. All information in the form of a data message must be given due evidential weight (Section 15(2)). Section 15(3) requires that in assessing the evidential weight of a data message, regard must be had to the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the data message was maintained; the manner in which its originator was identified; and any other relevant factor.

Retention: where the law requires that information to be retained, Section 16 states that that requirement is met by retaining the information in the form of a data message if the information contained in the data message is accessible so as to be usable for subsequent reference and the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and the origin and destination of that data message and the date and time it was sent or received can be determined.

Production of document or information: Section 17(1) states that where a law requires a person to produce a document or information, this requirement is met if the person produces, by means of a data message, an electronic form of that document or information.⁵⁶⁸

Notarisation, acknowledgement and certification: As per Section 18(1), where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, this requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

In the case where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, this requirement is met if the person provides a print-out certified to be a true reproduction of the document or information (Section 18(2)).⁵⁶⁹

Variation by agreement between parties: Sections 21 to 26 of the Act only apply if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for therein.

Formation and validity of agreements: In terms of Section 22(1), agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

Importantly, an agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror (Section 22(2)).

⁵⁶⁸ The integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for, the addition of any endorsement: or any immaterial change, which arises in the normal course of communication, storage or display.

⁵⁶⁹ Additionally, as per Section 18(3) of the Electronic Communications and Transactions Act, 2002 where a law permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Time and place of communications, dispatch and receipt: As per Section 23, a data message used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee. The data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee. Additionally, a data message must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

Expression of intent or other statement: An expression of intent or other statement, between the originator and the addressee of a data message is not without legal force and effect merely on the grounds that it is in the form of a data message or it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred (Section 24).

Attribution of data messages to originator: In terms of Section 25, a data message is that of the originator if it was sent by either the originator personally or a person who had authority to act on behalf of the originator in respect of that data message. A data message is also that of the originator if it was sent by an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

Acknowledgement of receipt of data message: Section 26 states that an acknowledgement of receipt of a data message is not necessary to give legal effect to that message. An acknowledgement of receipt may be given by any communication by the addressee, whether automated or otherwise, or by any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

CHAPTER V CRYPTOGRAPHY PROVIDERS

Register of cryptography providers: Section 29(1) requires the Director-General to establish and maintain a register of cryptography providers.⁵⁷⁰ The Director-General must, as per Section 29(2), record the following particulars in respect of a cryptography provider in that register:

- The name and address of the cryptography provider;
- a description of the type of cryptography service or cryptography product being provided; and
- such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately.⁵⁷¹

⁵⁷⁰ A "cryptography provider" is defined as any person who provides or who proposes to provide cryptography services or products in the Republic. Cryptography products are any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring a) that such data can be accessed only by relevant persons; b) the authenticity of the data; c) the integrity of the data; or d) that the source of the data can be correctly ascertained.

⁵⁷¹ A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

Registration with Department: Section 30 states that no person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 29 in respect of that person have been recorded in the register. Cryptography providers must in the prescribed manner, furnish the Director-General with the information required and pay the prescribed administrative fee.

A cryptography service or cryptography product is regarded as being provided in the Republic if it is provided from premises in the Republic, to a person who is present in the Republic when that person makes use of the service or product; or to a person who uses the service or product for the purposes of a business carried on in the Republic or from premises in the Republic.

Restrictions on disclosure of information: Section 31(1) prohibits the information contained in the register from being disclosed to any person other than to employees of the Department who are responsible for the keeping of the register. However, Section 31(1) does not apply in respect of information which is disclosed to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings, to government agencies responsible for safety and security in the Republic, pursuant to an official request, to a cyber-inspector, pursuant to section 11 or 30 of the Promotion of Access to Information Act 2 of 2000, or for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

CHAPTER VI AUTHENTICATION SERVICE PROVIDERS

Appointment of Accreditation Authority and other officers: The Director-General must act as the Accreditation Authority. The Accreditation Authority, after consultation with the Minister, may appoint employees of the Department as Deputy Accreditation Authorities and officers (Section 34).

Accreditation to be voluntary: Section 35 states that, subject to section 30, a person may, without the prior authority of any other person, sell or provide authentication products or services in the Republic.

Powers and duties of Accreditation Authority: Section 36(1) of the Act sets out the powers and duties of the Accreditation Authority which are listed as follows:

- monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act;
- temporarily suspend or revoke the accreditation of an authentication product or service; and
- appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act.

Section 36(2) requires the Accreditation Authority to maintain a publicly accessible database in respect of:

- authentication products or services accredited in terms of section 37;
- authentication products and services recognised in terms of section 40;

- revoked accreditations or recognitions; and
- such other information as may be prescribed.

Accreditation of authentication products and services in support of advanced electronic signatures: The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures (Section 37(1)). As required by Section 37(2), an application for accreditation must be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and be accompanied by a non-refundable prescribed fee.⁵⁷²

Criteria for accreditation of authentication products and services: Section 38 sets out several criteria for accreditation of authentication products and services. Specifically, in terms of Section 38(1), the Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that a number of criteria are met. These criteria are summarised in Table 46 below.

Table 46: Criteria for Accreditation of Authentication Products and Services

Article	Criteria
Article 38(1)	The electronic signature to which such authentication products or services relate must be: <ol style="list-style-type: none"> uniquely linked to the user; capable of identifying that user; created using means that can be maintained under the sole control of that user; linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable and based on the face-to-face identification of the user.
Article 38(2)	The Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services: <ol style="list-style-type: none"> Its financial and human resources, including its assets; the quality of its hardware and software systems; its procedures for processing of products or services; the availability of information to third parties relying on the authentication product or service; the regularity and extent of audits by an independent body; the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and any other relevant factor which may be prescribed.
Article 38(3)	Hardware and software systems and procedures must at least: <ol style="list-style-type: none"> be reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability and correct operation; be reasonably suited to performing their intended functions; and adhere to generally accepted security procedures.
Article 38(4)	The Accreditation Authority may stipulate, prior to accrediting authentication products or services: <ol style="list-style-type: none"> the technical and other requirements which certificates must meet;

⁵⁷² A person who falsely states that its products or services are accredited by the Accreditation Authority is guilty of an offence.

	<ul style="list-style-type: none"> b) the requirements for issuing certificates; c) the requirements for certification practice statements; d) the responsibilities of the certification service provider; e) the liability of the certification service provider; f) the records to be kept and the manner in which and length of time for which they must be kept; g) requirements as to adequate certificate suspension and revocation procedures; and h) requirements as to adequate notification procedures relating to certificate 1 suspension and revocation.
--	--

Revocation or termination of accreditation: Section 39 empowers the Accreditation Authority to suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40.

Accreditation of foreign products and services: The Minister may, by notice in the Gazette and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction (Section 40(1)).⁵⁷³

Accreditation regulations: In terms of Section 41, the Minister may make Regulations in respect of a) the rights and obligations of persons relating to the provision of accredited products and services; b) the manner in which the Accreditation Authority must administer and supervise compliance with those obligations; c) the procedure pertaining to the granting, suspension and revocation of accreditation; d) fees to be paid; e) information security requirements or guidelines; and f) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter.

CHAPTER VII CONSUMER PROTECTION

Information to be provided: Section 43 (1) required that a supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the information summarised in Table 47 below available to consumers on the web site where such goods or services are offered.

Table 47: Information to be provided to Consumers

Section	Information Requirement
43(1)(a)	Its full name and legal status.
43(1)(b)	Its physical address and telephone number.
43(1)(c)	Its web site address and e-mail address.
43(1)(d)	Membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body.
43(1)(e)	Any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer.
43(1)(f)	In the case of a legal person, its registration number, the names of its office bearers and its place of registration.

⁵⁷³ An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection 40(1), is guilty of an offence.

43(1)(g)	The physical address where that supplier will receive legal service of documents.
43(1)(h)	A sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;
43(1)(i)	The full price of the goods or services, including transport costs, taxes and any other fees or costs.
43(1)(j)	The manner of payment.
43(1)(k)	Any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers.
43(1)(l)	The time within which the goods will be dispatched or delivered or within which the services will be rendered.
43(1)(m)	The manner and period within which consumers can access and maintain a full record of the transaction.
43(1)(n)	The return, exchange and refund policy of that supplier.
43(1)(o)	Any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer.
43(1)(p)	The security procedures and privacy policy of that supplier in respect of payment, payment information and personal information.
43(1)(q)	Where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently.
43(1)(r)	The rights of consumers in terms of section 44, where applicable.

Section 43(2) requires the supplier to give the consumer the opportunity to review the entire electronic transaction, to correct any mistakes and to withdraw from the transaction, before finally placing any order.

If a supplier fails to comply with the provisions of Section 43(1) or 43(2), the consumer has the right to cancel the transaction within 14 days of receiving the goods or services under the transaction. If a transaction is cancelled in terms of Section 43(3), the consumer must return the performance of the supplier or, where applicable, cease using the services performed and the supplier must refund all payments made by the consumer minus the direct cost of returning the goods.

Section 43(5) requires the supplier to utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.⁵⁷⁴

Unsolicited goods, services or communications: Any person, who sends unsolicited commercial communications to consumers, must. As per Section 45(1) provide the consumer with the option to cancel his or her subscription to the mailing list of that person and with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer. Importantly, no agreement is concluded where a consumer has failed to respond to an unsolicited communication.⁵⁷⁵

⁵⁷⁴ The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

⁵⁷⁵ Any person who fails to comply with or contravenes Section 45(1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1). Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

CHAPTER VIII PROTECTION OF PERSONAL INFORMATION

Principles for electronically collecting personal information: Article 51(1) requires a data controller to have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law. In terms of Section 51(2), a data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required. The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored (Section 51(3)). Several other principles apply to the electronic collection of personal information. These are:

- The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law (Section 51(5));
- The data controller must, for as long as the personal information is used and for a period of at (cast one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected (Section 51(5));
- A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject(Section 51(6);
- The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed (Section 51(7));
- The data controller must delete or destroy all personal information which has become obsolete (Section 51(8));
- A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party (Section 51(9)).

6.2 Level of Compliance SADC Member States Act with International Best Practice

For the purpose of this comparative exercise, the UNCITRAL Model Law on Electronic Commerce (1996), and the South African Electronic Communications and Transactions Act, 2002⁵⁷⁶ have been selected as the benchmark for electronic transactions and electronic signature law. As represented in Table 48 below, the content of the Draft Bills currently on the table in Botswana, Malawi and Tanzania are unknown quantities due to the Bills not being available for public comment at this time. At the time of the preparation and publication of this report, the Botswana, Malawi and Tanzania’s draft Bills were not available for public comment.

Table 48: International and Regional Best Practice Electronic Communications and Transactions

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW
UNCITRAL Model Law on Electronic Commerce														

⁵⁷⁶ Act 25 of 2002.

Legal recognition of data messages	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Incorporation by reference	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Where the law requires information to be in writing , that requirement is met by a data message	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Where the law requires a signature of a person, that requirement is met in relation to a data message if a method is used to identify that person and to indicate that person's approval of the information contained in the data message	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Where the law requires information to be presented in or retained in its original form, that requirement is met by a data message if there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its original form, as a data message or otherwise	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Admissibility and evidential weight of data messages	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Retention of data messages: where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages provided that the information contained is accessible and usable for subsequent reference; data message is retained in the format in which it was generated, sent or received; information is retained as to enable the identification of the origin and destination of the data message and the date / time when it was sent or received.	x	P(A)	✓	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Formation and validity of contracts : an offer and acceptance of an offer may be expressed by means of data messages. ⁵⁷⁷	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Recognition of parties of data messages: a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x

⁵⁷⁷ Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

Attribution of data messages ⁵⁷⁸	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Acknowledgement of receipt: the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
South Africa's ECTA														
Register of cryptography providers to be established and maintained	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Cryptography service providers that provide cryptography services must register	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
The information contained in the register must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register unless required by law	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Accreditation Authority to maintain a publicly accessible database in respect of: authentication products or services accredited, authentication products and services recognised and revoked accreditations or recognitions	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Criteria for accreditation of authentication products and services must be set out in law	x	P(A)	x ⁵⁷⁹	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Accreditation Authority to suspend or revoke an accreditation if it is satisfied that the authentication service provider	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x

⁵⁷⁸ A data message is that of the originator if it was sent by the originator itself. As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent: (a) by a person who had the authority to act on behalf of the originator in respect of that data message; or (b) by an information system programmed by, or on behalf of, the originator to operate automatically. As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if: (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

⁵⁷⁹ Article 66 of the DRC's Draft Law requires that "an institution that would like to set up or operate an electronic certification system as part of payment transactions must first get approval from the Central Bank. The latter determined through guidelines, the institution conditions of approval, suspension and withdrawal." It is not clear what is meant in the law by "electronic certification system" and this is not defined.

has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted														
Recognition of the accreditation of foreign authentication products or services	x	P(A)	x	x	P(A)	✓	x	●	✓	✓	x	P(A)	✓	x
Consumer protection: Law to specify the information to be provided by a supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction	x	P(A)	x	x	P(A)	✓	x	●	x	✓	x	P(A)	✓	x
Consumer must be given the opportunity to review the entire electronic transaction, to correct any mistakes and to withdraw from the transaction, before finally placing any order.	x	P(A)	x	x	P(A)	✓	x	●	x	✓	x	P(A)	✓	x
Data protection: a data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject	x	P(A)	x	x	P(A)	✓	x	x	x	✓	x	P(A)	✓	x
A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required	x	P(A)	x	x	P(A)	✓	x	x	x	✓	x	P(A)	✓	x

SECTION 7: ELECTRONIC MONEY

7.1 The Current State of Play in SADC

The emergence of new electronic technologies has resulted in the introduction of new and innovative payment products and services. Advances in Information and Communications Technology (ICT) will continuously influence the payments environment. It is essential for Central Banks to take note of these developments and ensure that appropriate and fit-for-purpose legal provisions are put in place.

Electronic Money (E-Money) has the potential to fundamentally transform the payments domain. It is advisable for all countries in SADC to introduce legislation that regulates the issuance and usage of E-Money. It is however essential that the E-Money regulatory framework is technology neutral and does not constrain itself

to a particular form factor or technology platform. The approach adopted by UNCITRAL in the drafting of the UNCITRAL Model Law on Electronic Commerce is recommended in the regard.⁵⁸⁰

Smart card-based E-Money schemes have been launched and are operating in many countries around the world. Network-based or software-based E-Money schemes have been less rapid in their expansion but are nevertheless significant in the payments regulatory environment.

Mobile phone technology is an ideal technology platform to introduce payment products and services. The phenomenal growth experienced by the mobile phone industry together with the mobile phone networks' desire to introduce additional value added services for their clients, has resulted in the emergence of so-called Mobile Money products and services. Mobile Money should however not be regulated in isolation and should be a subset of the bigger E-Money regulatory framework.

As represented in Table 49 below, there are only two SADC Member States that have issued a legally binding Directive / Determination on E-Money. The DRC's Directive No. 24 on the Issuance of Electronic Money and Electronic Money Issuing Institutions very closely resembles the European Commission Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions as does Namibia's Payment System Determination (PSD - 3) Determination on Issuing of Electronic Money which was issued in 2012. Both of these are excellent regulatory instruments on a par with the international best practice statutory instrument selected for the comparative exercise profiled in this report. It is strongly recommended that (PSD - 3) Determination on Issuing of Electronic Money and Directive No. 24 on the Issuance of Electronic Money and Electronic Money Issuing Institutions be considered as appropriate benchmarks for other SADC Member States.

⁵⁸⁰ The UNCITRAL Model Law is technologically neutral as it does not depend on or presuppose the use of any particular type of technology and could be applied to the communication and storage of all types of information. See United Nations Commission on International Trade Law (UNCITRAL) 2009 *Promoting Confidence in Electronic Commerce: Legal Issues on International use of Electronic Authentication and Signature Methods* 37 where it is stated that, "Technological neutrality is particularly important in view of speed of technological innovation and helps to ensure that legislation remains capable of accommodating future developments and does not become obsolete too quickly. Accordingly, the Model Law carefully avoids any reference to particular technical methods of transmission or storage of information."

Table 49: Level of Development of E-Money Regulatory Frameworks in SADC Member States

E-MONEY REGULATORY FRAMEWORK	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW
E-Money Regulations	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E-Money Directives	x	x	✓	x	x	x	x	✓	x	x	x	x	●	x
E-Money Guidelines	x	x	x	x ⁵⁸¹	x	x	x	✓	x	x	x	✓ ⁵⁸²	x	●
E-Money Position Paper	x	● ⁵⁸³	x	x	x	x	x	x	x	✓	x	* ⁵⁸⁴	x	x

The South African Reserve Bank has not issued E-Money Regulations of Directives. However, the South African Reserve Bank’s position on E-Money is set out in Position Paper NPS 01/2009 on Electronic Money. As noted on the South African Reserve Bank website, Position Papers are “published by the South African Reserve Bank in order to state the Reserve Bank’s position in respect of specific payment system issues. These documents normally contain approaches, procedures and policy matters, which are applicable at a particular time.”

Several SADC countries are currently engaged in the drafting of E-Money Guidelines and or Policy Papers. The IMF is currently assisting Botswana with the drafting of an E-Money Policy Paper and the Reserve Bank of Zimbabwe is working on an E-Money / Electronic Payments Guideline. In an interview held with the Bank of Zambia in February, 2013, we were informed that the Bank of Zambia are about to issue new Electronic Money Directives. We were unfortunately not provided with a copy at the time of the in-country visit.

Malawi has not issued E-Money Regulations, nor has the RMB issued a Directive or Guideline. The National Payment System Bill does however contain several provisions that refer specifically to E-Money. These include Article 12(1) that states, “no person shall establish or operate any payment, clearing and settlement system or services, remittance services including electronic money transfer services, mobile payment services or issue payment instruments without licence or prior authorisation from the Reserve Bank” and Article 3(1)(b) that reads, “the Principal object of this Bill is to provide for the regulation of inter alia, payment, clearing and settlement systems, mobile payment systems, payment instruments, remittance service providers, electronic money transfers, card issuers, travellers cheques agencies.”

⁵⁸¹ In the introduction to the Central Bank of Lesotho National Payment System Division Guidelines on Mobile Money, the Central Bank of Lesotho appears to have equated mobile money with electronic money. This is evidenced by the following statement, “Mobile money in Lesotho includes various components that facilitate the delivery of payments to the banked and non-banked population through mobile phones or other similar electronic means. Mobile money can be issued in different forms, such as card-based (e.g. prepaid card) and network-based which can be accessed via the internet, mobile phones or any other similar devices. Electronic money (mobile money) is a payment instrument that contains monetary value that is paid in advance by the user to the mobile money issuer. The user of mobile money can undertake payments for purchases of goods and services to agents who accept the mobile money as payment.”

⁵⁸² Guidelines, the Guidelines on Introduction and Operation of Auditable Card Based Electronic Money Schemes in Tanzania

⁵⁸³ The IMF is currently assisting Botswana with the preparation of an E-Money Policy Paper.

⁵⁸⁴ The position of the BOT with respect to E-Money is included in the Guidelines on Introduction and Operation of Auditable Card Based Electronic Money Schemes in Tanzania.

Electronic currency institutions are defined in Article 2(i) of Law 15/99 of 1 November Law on Credit Institutions and Finance Companies (As Amended), as credit institutions whose main purpose is to issue payment instruments in electronic form, under terms established in applicable legislation. Electronic currency is understood to mean the monetary value represented by a credit right against the issuer, which is stored on an electronic medium and accepted in payment by entities other than the issuer. Article 3(g) lists electronic currency institutions as credit institutions. Mozambique has however not issued E-Money Regulations, nor has the *Banco de Moçambique* issued a Directive or Guideline on the subject.

The Central Bank of Swaziland has not issued E-Money regulations or specific E-Money guidelines. The Bank's position with respect to E-Money is however set out in paragraph 3.0 of the Minimum Standards for Electronic Payment Schemes, issued by the Central Bank of Swaziland in 2010 pursuant to the power conferred on it by sections 4(f) and 42(b) of the Central Bank of Swaziland Order 1974 (as amended). Paragraph 3.0 states that, "the Bank considers E-Money to be a supplement to physical notes and coin, particularly in the long-run." These words appear to be copied directly from the South African Reserve Bank Position Paper on Electronic Money. In order to facilitate the development of E-Money products and opportunities they present on a national and regional basis, the Bank commits itself in paragraph 3.0 to support the development of a banking industry's vision for electronic substitutes for physical bank notes and coins and paper based instruments (such as cheques); support the development of national standards to enable interoperability of e-money schemes; products and devices; and participate in initiatives aimed at providing secure payment instruments for the general public, including the unbanked and rural communities of Swaziland.

While the Minimum Standards for Electronic Payment Schemes document provides general statements pertaining to all "electronic payment schemes", it does not provide specifics with respect to E-Money. In particular, no detail is provided on authorisation to issue E-Money in Swaziland, specific requirements for issuing E-Money, general conditions for using agents to provide E-Money services, E-Money transaction and balance limits, minimum capital requirements, E-Money risk mitigation requirements, E-Money reporting requirements or AML/CFT measures.

7.2 The Scope and Content of Namibia's Payment System Determination (PSD-3)

Namibia is only one of two SADC countries to have issued a legally enforceable instrument on electronic money. The Payment System Determination (PSD - 3) Determination on Issuing of Electronic Money was issued in 2012 by the Governor of the Bank of Namibia (The Bank) under the powers vested in the Bank by virtue of Section 14 of the Payment System Management Act, 2003 (As Amended).⁵⁸⁵ The Determination applies to all persons who intend to issue E-Money in Namibia in terms of Section 5 of the Payment System Management Act, 2003. Both banks and non-bank actors are permitted to apply for authorisation to issue E-Money. Permission to offer specific E-Money-related services is subject to authorisation by the Bank. In terms of Regulation 14.1 however, non-bank E-Money issuers are limited to the provision of e-money services only and may not engage in any activities other than issuing E-Money and providing services related to the issuance of E-Money. Any party (other than a banking institution) that wishes to offer E-Money services in addition to other services must establish a separate entity whose activities will be limited to the issuance of E-Money and the provision of related services. The Bank may consider requests for a waiver from this requirement in exceptional circumstances.⁵⁸⁶

⁵⁸⁵ Act 18 of 2003 (As Amended).

⁵⁸⁶ To receive a waiver, an E-Money issuer must prove that compliance with such a requirement would be unduly burdensome and that granting a waiver would not compromise the Bank's ability to effectively supervise the E-Money issuer.

In addition to PSD – 3, the Bank of Namibia issued Guidelines for Issuance of Electronic Money and other Payment Instruments in Namibia in March 2012.

For the purpose of providing a frame of reference for other countries that may be considering issuing an E-Money Directive or making amendment to the National Payment System Act to include salient provisions, the scope and content of the provisions found in the PSD-3 are set out below.

The substantive provisions found in Payment System Determination (PSD - 3) Determination on Issuing of Electronic Money are set out below.

Definition of E-Money: Regulation 3.7 defines E-Money as, “a designated payment instrument which has monetary value as represented by a claim on its issuer, that is: stored electronically, issued on receipt of funds, accepted as a means of payment by persons other than the issuer, and is redeemable upon demand for cash denominated in Namibian Dollars.

The Guidelines for Issuance of Electronic Money and other Payment Instruments in Namibia, 2012 provide a useful description of E-Money service and types of accounts. These are summarised below for reference purposes as these descriptions may be useful to other Central Banks in the SADC region that are considering issuing E-Money Regulations and or Guidance Notes.

E-Money services include the following:

- Opening an electronic money account;
- Loading value onto an electronic wallet (Cash-in);
- Redeeming value from an electronic wallet (Cash-out);
- Paying bills;
- Sending domestic money transfers;
- Receiving / disbursing domestic money transfers.⁵⁸⁷

The different types of E-Money accounts are summarised in Table 50 below.

Table 50: Types of E-Money Accounts

Ref.	Type of Account	Description
4.2.1	Individual Accounts	These are intended to be used by individuals.
4.2.2	Business Accounts	These are designed for businesses, organisations and government entities and are used for a number of payment-related services including: <ul style="list-style-type: none"> • Payment of salaries or social benefits by government (G2P); • Payment of salaries or fees by businesses (B2P); • Payment of goods received or services rendered (B2B or C2B);
4.2.3	Agent Accounts	These are designed to facilitate the transfer and usage of E-Money funds and accounts. As agents perform a number of functions on behalf of the E-Money issuer, higher transaction and balance limits

⁵⁸⁷ Paragraph 4.1 of the Guidelines for Issuance of Electronic Money and other Payment Instruments in Namibia, 2012

	are necessary in order to provide sufficient liquidity.
--	---

Authorisation to issue electronic money in Namibia: Any entity wishing to issue E-Money in Namibia is required to apply to the Bank for authorisation. An application for authorisation must include all documents, data, or other information as prescribed by the Bank.⁵⁸⁸ Such authorisation may be suspended (Regulation 18) or cancelled (Regulation 19) under the circumstances summarised in Table 51 below.

Table 51: Suspension and Cancellation of Authorisation

Reg.	Suspension	Reg.	Cancellation
18.1	The Bank will suspend an authorisation to issue E-Money under any of the following circumstances where: ⁵⁸⁹	19.1	The Bank may cancel an authorisation to issue E-Money under the following circumstances: ⁵⁹⁰
18.1.1	The owner is carrying on business in a manner which is detrimental to the stability of the National Payment System, or is incapable of providing services as per agreed service level standards	19.1.1	The owner fails to comply with this determination and remedial measures required by the Bank following an inspection of the affairs of the E-Money issuer
18.1.2	There is a violation of any of the provisions of the determination or any other applicable laws or regulations; and/or any other circumstances which the Bank may consider material to warrant suspension	19.1.2	It is determined that an authorisation was obtained on the strength of misrepresented, inaccurate, or misleading information furnished to the Bank at the time of application
		19.1.3	There is a violation of any of the provisions of this determination, the Payment System Management Act, 2003 (As Amended) or any other applicable laws or regulations
		19.1.4	The scheme is considered not to be conducive to the national interest of Namibia
		19.1.5	The E-Money Issuer ceases to operate or becomes insolvent
		19.1.6	Any other circumstances which the Bank may consider material to warrant cancellation

Licence Renewal: An E-Money issuer's license to issue E-Money must be renewed annually upon payment of the required fees, provided that the E-Money issuer is in full compliance with the requirements of the Determination.⁵⁹¹

⁵⁸⁸ Regulation 9.1 of PSD – 3. The authorised E-Money institutions in Namibia are MobiPay and Nam-mic Payment Solutions.

⁵⁸⁹ The Bank of Namibia will ensure that all due diligence processes are followed before suspension of an E-Money issuer is instituted.

⁵⁹⁰ The Bank of Namibia shall ensure that all due diligence processes are followed before cancellation of an authorisation to issue E-Money is instituted.

⁵⁹¹ Regulation 9.2 of PSD – 3.

Notification of Significant Changes to E-Money Services: Regulation 9.3 requires E-Money issuers to notify the Bank of any significant proposed change to the scope or nature of the E-Money services provided. Such notification must be provided at least 30 days prior to the date on which the change is to take effect. The Regulation provides several examples of significant changes including: a change in electronic delivery mechanism used to provide services; a in partnerships used to provide services; a large increase in transaction volume (e.g. through contract to provide payment services to a large company or government entity); a large increase in the size of agent network.⁵⁹²

General conditions for using agents to provide electronic money services: these are set out in Regulation 10 of PSD – 03. Issuers of E-Money may offer any or all approved E-Money services through agents acting on their behalf, provided that issuers comply with all provisions in the Determination relating to the use of agents. If using an agent, the E-Money issuer is held fully responsible and liable for ensuring that the agent complies with all legal and regulatory requirements related to the provision of E-Money services. In terms of Regulation 10.2, prior to establishing agreements with specific agents with respect to the provision of E-Money services, e-money issuers must be able to offer services through agents safely and effectively. The Regulation states further that, “the Bank shall prescribe a list of required actions to be taken before notifying the Bank of an e-money issuer’s intention to offer services through agents.” Importantly, in terms of Regulation 10.3, an e-money issuer that has met the general conditions for offering E-Money services through agents may submit a notification to the Bank of its intention to contract a specific agent or agents to provide services on its behalf.⁵⁹³

Specific requirements for issuing E-Money in Namibia: Regulation 11 sets out several specific requirements for the issuing of E-Money in Namibia. These are summarised in Table 52 below.

Table 52: Specific Requirements for Issuing E-Money in Namibia

Reg.	Requirement	Detail
11.1	Characteristics of E-Money	E-Money issuers must ensure that e-money schemes abide with the following:
11.1.1	No interest and redemption at par value	E-Money issuers may not pay interest or other compensation to customers for funds held in electronic wallets. E-Money shall be redeemed at par value.
11.1.2	Transaction and balance limits	Electronic wallets are subject to transaction and balance limits, as provided in a Circular that will be issued by the Bank.
11.1.3	Funds are not deposits	Customer funds held on electronic wallets are not deposits, and acceptance of customer funds by E-Money issuers shall not constitute deposit-taking. Customer funds shall be treated as “accounts payable” for accounting purposes.
11.1.4	No credit or	E-Money issuers are not permitted to offer credit or otherwise

⁵⁹² If the Bank has any objections or concerns with respect to the proposed change, it will communicate these concerns to the E-Money issuer within 30 days of receipt of notification. In such an event, the E-Money issuer shall not proceed with the change until and unless it receives the Banks approval.

⁵⁹³ The Regulation reads further that, “the Bank shall prescribe the information that must be included with this notification, which must be submitted at least 14 days prior to the proposed date for commencement of services.”

	intermediation of funds	intermediate customer funds. E-Money issuers are not permitted to engage in banking business, and they are only permitted to deposit customer funds in pooled deposit accounts, as described in this Determination.
11.2	Safe storage of customer funds	In order to ensure that customer funds are protected against loss, E-Money issuers shall be required to comply with the following requirements:
11.2.1	Funds must be pooled and deposited in accounts with a licensed Namibian bank	E-Money funds received from customers and agents must be pooled and deposited in accounts with one or more licensed Namibian banking institutions.
11.2.2	Funds held in trust and protected from creditor's claims in the event of insolvency	Pooled funds must be held in trust on behalf of the customers and agents of the E-Money issuer. Pooled funds held in trust must be legally protected from creditors' claims in the event of insolvency.
11.2.3	Pooled funds may only be used to fund customer and agent transactions	Except with respect to interest paid under the conditions described below, pooled funds may only be used to fund customer and agent transactions, such as redemptions or other transactions that result in a net reduction in the value of outstanding E-Money liabilities.
11.2.4	Aggregate value of pooled funds must equal the value of all outstanding E-Money liabilities	At all times, the aggregate value of the pooled funds must equal at least 100% of the value of all outstanding E-Money liabilities. These funds shall be reconciled on a daily basis, with any deficiencies addressed within one business day.
11.2.5	Issuers may earn interest on pooled funds	E-Money issuers are permitted to earn interest on pooled funds. However, issuers may only withdraw interest earned (or use interest to pay fees or charges related to the administration of the pooled account) if the remaining aggregate value of the pooled funds would equal at least 100% of the value of all outstanding E-Money liabilities.
11.2.6	The Bank may waive or modify requirements	The Bank reserves the right to waive or modify one or more of the aforementioned requirements in exceptional circumstances, when in the Bank's sole determination: <ul style="list-style-type: none"> • compliance with a requirement would be unduly burdensome; and • waiver or modification of such a requirement would not affect the safety of customer funds.
11.3	Transaction and balance limits	Individual accounts, business accounts, and agent accounts are subject to transaction and balance limits, as may be determined by the Bank from time to time. In establishing these limits, the Bank will consider factors such as: <ul style="list-style-type: none"> • Customer needs; • Market and economic conditions; • Money laundering and terrorist financing risk; • Other risk mitigation measures taken by E-Money issuer(s); and • Any other relevant factors.

Transaction and Balance Limits: Transaction and Balance Limits are set in Circular PSMA 1 Transaction and Balance Limits for Electronic Money Accounts and Fees Payable that was issued on in March 2012. It is important to note that as stated in paragraph 3 of the Circular, “limits are cumulative for aggregate outbound transactions (i.e. transactions on which funds are deducted from the customer’s account, such as cash out, bill payment, or outgoing money transfer.) If a customer has more than one E-Money account with a single issuer, the issuer must ensure that the aggregate value of all transactions/balances on all the customer’s accounts does not exceed the transaction and balance limits.” The transaction limits as set out in the Circular are presented in Table 53 below.

Table 53: Transaction Limits

Type of Account	Outbound Limit Per Transaction	Outbound Limit Per Day	Outbound Limit Per Month	Outbound Limit Per Year	Maximum Balance
Individual Accounts	N\$ 4,000	N\$ 4,000	N\$ 20,000	N\$ 100,000	N\$ 10,000
Business Accounts	To be determined by E-Money issuer and business, subject to the Bank’s approval.				
Agent Accounts	To be determined by E-Money issuer and business, subject to the Bank’s approval.				

Fees Payable: As per paragraph 5 of Circular PSMA 1, the fees set out in Table 54 below are payable by E-Money issuers. All fees are mandatory and refundable.

Table 54: Fees Payable by E-Money Issuers

Type	Amount in N\$
Application to provide E-Money services	N\$ 5,000
Authorisation to provide E-Money services	N\$ 10,000
Annual license renewal fee	N\$ 5,000

Minimum Capital Requirements: These are set in Regulation 11.4. E-Money issuers are required to comply with the following initial and ongoing minimum capital requirements:

Table 55: Initial and Ongoing Capital Requirements

Initial Requirement	Ongoing Requirement
N\$ 2.5 million	The greater of: (i) N\$2.5 million; or (ii) of outstanding electronic money liabilities. ⁵⁹⁴

⁵⁹⁴ For the purposes of calculating “outstanding electronic money liabilities”, the E-Money issuer is required to use the greater of: (i) outstanding electronic money liabilities at the end of the prior business day; or (ii) average outstanding electronic money liabilities over the previous six months.

In terms of Regulation 11.4.2, the Bank may on application in writing and on good cause shown, in writing permit an E-Money issuer to, for such limited period of time as the Bank may specify, have capital funds which are lower than the capital funds determined under section 11.4.1 of this Determination and determine that the capital requirements of an E-Money issuer shall, on a consolidated basis, apply to, and the capital be reflected in the consolidated accounts of, the E-Money issuer, its holding company or the affiliate or associate of the E-Money issuer or its holding company.

Anti-Money Laundering & Combating the Financing of Terrorism (AML/CFT): As accountable institutions under the FIA, E-Money issuers are responsible for ensuring that e-money payment instruments are not misused for money laundering, terrorist financing, or other “unlawful activity” regulated under the FIA and its accompanying regulations. E-Money issuers must fully comply with Customer Due Diligence (CDD) and all other requirements under the FIA and its accompanying regulations. In addition, if E-Money issuers wish to offer certain services via agents, they are required to train their agents to perform CDD and maintain records on their behalf. E-Money issuers must monitor their agents to ensure compliance with the FIA and its accompanying regulations.

Risk Management and Mitigation: These requirements are set out in Regulation 12 and cover Mitigation of Key Risks (Regulation 12.1); Customer Protection (Regulation 12.2); and Real-time Transactions (Regulation 12.3). Regulation 12.1 requires E-Money issuers to comply with risk mitigation measures as prescribed by the Bank. In terms of Regulation 12.2, E-Money issuers must take steps to ensure that customers understand the services which they are using - including the inherent risks of using such services - and are protected from fraud and other forms of customer abuse. In addition, the roles, responsibilities, and rights of all parties must be clearly communicated. The Bank shall prescribe specific requirements in respect to disclosure and customer protection. To avoid settlement risk, Regulation 12.3 requires all E-Money transactions affecting the value held on an e-wallet to be processed in real time. No delay is permitted between when the e-wallet of the payer is debited and when the e-wallet of the payee is credited.

Written Contracts: All E-Money issuers must ensure that agreements with agents and service providers are governed by written contracts. Paragraph 9 of the Guidelines for Issuance of Electronic Money and other Payment Instruments in Namibia, 2012 provides guidance on the minimum requirements for contracts with agents and service providers. These contracts should include provisions addressing inter alia:

- Clarification of roles, responsibilities and contractual liabilities of the parties;
- Responsibilities of the parties for providing and receiving information;
- Materiality thresholds and procedures for notifying the issuer of service disruptions, security threats or other issues that create material risks;
- Ownership and protection on consumer data, transaction data and other information;
- Whether agents and service providers are required to obtain insurance;
- Performance benchmarks;
- Termination or expiration of contracts, including circumstances leading to intervention by the issuer;
- Business continuity measures

- The issuers right to monitor and audit the agent or service provider’s operations, security policy and procedures and contingency plans; and
- The Bank of Namibia’s right to inspect data, documents, records and premises of the agent or service provider.

Competition and Interoperability of Electronic Money Services: Interoperability is not mandated at this point in time. The Bank however reserves the right in Regulation 15.2 to require interoperability and/or non-exclusivity at a future date, after providing E-Money issuers with notice and sufficient time to conform as determined by the Bank. E-Money issuers should ensure their ability to comply with such a mandate in a timely and cost-effective manner. E-Money issuers are however required to use technical standards and specifications that ensure that interoperability is feasible at low cost in the future.

Reporting requirements: E-Money issuers shall be required to submit reports as prescribed by the Bank. In order to ensure that it is able to effectively supervise E-Money issuers, the Bank reserves the right to inspect all E-Money-related records, data, or other relevant information, whether in the possession of the E-Money issuer or its agent(s).

Penalties: An E-Money issuer, person or entity that contravenes or otherwise fails to comply with the Determination will be subject to penalties as provided under the Payment System Management Act, 2003 (As Amended).⁵⁹⁵

7.3 Level of Compliance with International and Regional Best Practice

For the purpose of this comparative exercise, Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions has been selected as the benchmark for E-Money Regulations, Directives and Guidelines issued by SADC countries. In the section that follows, the DRC’s Directive No. 24 on the Issuance of Electronic Money and Electronic Money Issuing Institutions, Namibia’s Payment System Determination (PSD - 3) Determination on Issuing of Electronic Money, Tanzania’s Guidelines on Introduction and Operation of Auditable Card Based Electronic Money Schemes in Tanzania and South Africa’s E-Money Position Paper are measured against this standard in order to highlight similarities, gaps and substantial difference in interpretation.

Table 56: Level of Compliance with Best Practice (E-Money)

Best Practice Requirement	Ref	DRC		NA		RSA		TZ	
		In ⁵⁹⁶	C ⁵⁹⁷	In	C	In	C	In	C
Clearly defined definition of E-Money	Article 2(2)	✓	✓	✓	✓	✓	✗	✓	✗
E-Money does not constitute deposit taking & E-Money issuers may not take deposits	Recital 13 Article 6(2)	✓	✓	✓	✓	✗	✗	✗	✗
E-Money is an electronic surrogate for bank notes and coins	Recital 13			✗	✗	✗	✗	✓	✗ ⁵⁹⁸

⁵⁹⁵ Act 18 of 2003 (As Amended).

⁵⁹⁶ In = provision found in the Directive, Guideline or Position Paper.

⁵⁹⁷ C = level of compliance with Directive 2009/110/EC.

E-Money Institutions are not permitted to grant credit from the funds received or held for the purpose of issuing E-Money	Recital 13	✓	✓	✓	✓	✗	✗	✗	✗
E-Money issuers are not permitted to grant interest or any other benefit	Recital 13 Article 12	✓	✓	✓	✓	✗	✗	✗	✗
Conditions for authorisation should be proportionate to operational and financial risks	Recital 13	✓	✓	✓	✗ 599	✗	✗	✓	✗
Issuance of E-Money is limited to credit institutions, E-Money institutions, post office giro institutions, Bank, the European Central Bank or the central bank of another Member State, person that has been registered after qualifying as a small electronic money institution	Recital 17	✓	✓	✓	✓ 600	✓	✗ 601	✓	✗ 602
E-Money institution to inform competent authority in advance of any material change in measures to safeguard funds	Article 3(2)	✓	✓	✓	✓	✗	✗	✗	✗
E-Money institutions may distribute & redeem E-Money through natural or legal persons acting on their behalf	Article 3(4)	✓	✓	✓	✓	✗	✗	✗	✗
Initial capital	Article 4	✓	✓	✓	✓	✗	✗	✗	✗
Own funds	Article 5, 57 to 61, 63, 64 & 66	✓	✓			✗	✗	✗	✗
Safeguarding requirements	Article 7(1)	✓	✓	✓	✓	✗	✗	✗	✗
Optional Exemptions (Small E-Money Institutions) Requirements set out in Articles 3,4,5 and 7 if: <ul style="list-style-type: none"> total business activity does not exceed EUR500 000; none of natural persons responsible for 	Article 8	✗	✗	✗	✗	✗ 603	✗	✗	✗

⁵⁹⁸ The Tanzanian provision need to be looked at as E-Money is definitely not a substitute for “cheque, credit/debit card or account transfers provided each transaction is traceable from source to its finality” as is stated in the Tanzanian Guideline.

⁵⁹⁹ Proportionality not specifically referred to in PSD-3.

⁶⁰⁰ PSD-3 does not list the specific institutions that may issue E-Money. The approach adopted is rather to permit both banks and non-banks to apply for authorisation subject to a number of conditions including that non-bank E-Money issuers are limited to the provision of E-Money services only and may not engage in any activities other than issuing E-Money and providing services related to the issuance of E-Money. Any party (other than a banking institution) that wishes to offer E-Money services in addition to other services must establish a separate entity whose activities will be limited to the issuance of E-Money and the provision of related services. The Bank may consider requests for a waiver from this requirement in exceptional circumstances.

⁶⁰¹ Only banks may issue E-Money in South Africa. Non-banks may provide services as system operators or third-person payment service providers in terms of Directives 1 and 2 of 2007. This is very limiting and not in-line with Strategic Objective 1: of Vision 2015, namely that the South African Reserve Bank will continue to evaluate and improve the participation of non-bank stakeholders in the clearing system and/or in formal payment system management structures.

⁶⁰² See paragraph 8.1(iii) where the issuing of E-Money is limited to, “financial institutions alone or in collaboration with private non-financial institutions.”

⁶⁰³ Paragraph 11 does states that, “the South African Reserve Bank supports the approach and limits for particular classes of transactions published by the Financial Intelligence Centre.” This does not however equate to the recognition of different types / levels of E-Money Issuers.

management & operation of business have been convicted of AML/CFT offences; • Maximum storage amount on payment instrument / account is applicable									
E-Money must be issued at par value on receipt of funds	Article 11(1)	✓	✓	✓	✓	✓	✓	✗	✗
Contract to state conditions of redemption and fees and cardholder to be informed of conditions before being bound by the contract	Article 11(3)	✓	✓	✓	✓	✗	✗	✓	✗ 604
Redemption may be subject to a fee which must be stated in the contract and only in specific circumstances	Article 11(4)	✓	✓	✓	✓ 605	✗	✗	✓	✗ 606
Additional Provisions Included in the Namibian Payment System Determination (PSD - 3) Determination on Issuing of Electronic Money									
E-Money issuers license must be renewed annually	R9.2	✗	✗	✓	✓	✗	✗	✗	✗
E-Money issuer is held fully responsible and liable for ensuring that the agent complies with all legal and regulatory requirements related to the provision of E-Money services	R10	✓	✓	✓	✓	✗	✗	✗	✗
E-Money issuers that met the general conditions for offering E-Money services through agents may submit a notification to the Bank of its intention to contract a specific agent or agents to provide services on its behalf.	R10.3	✗	✗	✓	✓	✗	✗	✗	✗
Transaction limits are applicable	R11.3 & Circular PSMA 1	✗	✗	✓	✓	✗	✗	✗	✗
Competition and interoperability is not mandated but Bank reserves the right to mandate interoperability at a future date	R15.2	✗	✗	✓	✓	✓	✓	✓	✗ 607
Reporting requirements	R17	✗	✗	✓	✓	✗	✗	✗	✗

⁶⁰⁴ A timeframe is not set in the Tanzanian Guidelines.

⁶⁰⁵ Not specifically stated but implied through the normal interpretation of the wording of PSD-3.

⁶⁰⁶ The circumstances when a fee may be charged are not set out in the Tanzanian Guideline.

⁶⁰⁷ Interoperability is mandated in the Tanzanian Guideline. This may in-fact, at this stage be a negative influencer and stifle innovation. It may be better to suggest, as is the case in the Namibian PSD-3 that the Central Bank reserves the right to mandate interoperability at a later stage.

SECTION 8: PAYMENT SERVICES

Most SADC Member States do not have a well-structured legal and regulatory framework for retail payments. Vital issues such as electronic money (E-Money), card payments, agent banking, the authorisation of payment service providers (PSPs), the issuance of payment instruments and the rights and obligations of PSPs and users are generally poorly covered, if at all.

As noted in [section 3.2.2.5](#) of this report, “in recognition of the growing importance of retail payments and the need to harmonise domestic law in this area, the European Parliament and the Council adopted Directive 2007/64/EC Payment Services in the Internal Market (PSD) otherwise known as the Payment Services Directive in November 2007. Member States had until 1 November 2009 to transpose the Directive into National Law.” The PSD is the first piece of legislation that concretely deals with issues in the realm of PSPs and the users of their products. This Directive is a vital building block in the payments legal and regulatory framework and deals with several issues that have escaped regulatory attention for years. The PSD covers several of the principles set out in the [BIS/World Bank General Principles for International Remittance Services](#) including, Principle 1) Transparency and Consumer Protection;⁶⁰⁸ Principle 3) Legal and Regulatory Environment;⁶⁰⁹ and Principle 4) Market Structure and Competition.⁶¹⁰

It is also important to note that the PSD applies to payment services provided within the community. The payment services falling within the scope of the PSD are as follows:

- 1) services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
- 2) services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
- 3) execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:
 - execution of direct debits, including one-off direct debits;
 - execution of payment transactions through a payment card or a similar device;;
 - execution of credit transfers, including standing orders;
- 4) execution of payment transactions where the funds are covered by a credit line for a payment service user: execution of direct debits, including one-off direct debits;
 - execution of payment transactions through a payment card or a similar device;
 - execution of credit transfers, including standing orders;

⁶⁰⁸ Principle 1 of the *General Principles for International Remittance Services* requires that the market for remittance services should be transparent and have adequate consumer protection.

⁶⁰⁹ Principle 3 of the *General Principles for International Remittance Services* requires that remittance services should be supported by a sound and predictable, nondiscriminatory and proportionate legal and regulatory framework in relevant jurisdictions.

⁶¹⁰ Principle 3 of the *General Principles for International Remittance Services* requires that, “competitive market conditions, including appropriate access to domestic payment infrastructure should be fostered in the remittance industry.”

- 5) the issuing and/or acquiring of payment instruments;
- 6) money remittance; and
- 7) the execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

The EU PSD is applicable to all of the following payment service providers:

- **credit institutions** within the meaning of Article 4(1)(a) of Directive 2006/48/EC (Article 1(1)(a));
- **electronic money institutions** within the meaning of Article 1(3)(a) of Directive 2000/46/EC (Article 1(1)(b));
- **post office giro institutions** which are entitled under national law to provide payment services (Article 1(1)(c));
- **payment institutions** within the meaning of this Directive (Article 1(1)(d));
- **the European Central Bank and national central banks** when not acting in their capacity as monetary authority or other public authorities (Article 1(1)(e));
- **Member States or their regional or local authorities** when not acting in their capacity as public authorities (Article 1(1)(f)).

None of the 14 SADC Member States included in this study have a standalone piece of legislation or regulation in place that has the scope of application that the PSD has.

On the 1 November 2002, Aviso N° 01/2002 was issued in Angola under the powers set out in Article 3 of the Foreign Exchange Law, Law n° 5/97 of 27 June, and Articles 30 and 58 of the *Banco Nacional de Angola* Act -Law n° 6/97 of 11 July. Aviso N° 01/2002 regulates certain aspects related to the provision of payment services under the Payment System of Angola (SPA). Article 2 defines what is meant by a payment transaction and Article 3 defines a payment services as, "a systematic set of procedures provided by the service provider that enables the completion of a payment."

Article 4 states that the provisions of Aviso N° 01/2002 apply to the following payment services:

- "a) receipt by the service provider, or cash payment instrument from the sender to make a payment to the final beneficiary or his legal representative;
- b) the receipt by the service provider, invoice to be paid and the payment instrument and the delivery of those documents to the beneficiary's bank to make bank said final settlement and conclusion of payment to the final beneficiary stated on the invoice, or his legal representative;
- c) the availability of mechanisms of transmission to banks for electronic payment instructions under the Payments System of Angola."

These payment services may be provided by the following entities (Article 6):

- Banks and credit unions (Article 6(1)(a));
- Financial corporations, in accordance with the regulations of their activity (Article 6(1)(b));
- The Postal Administration, according to the Postal Law (Article 6(1)(c));
- Legal non-financial persons, authorised by the National Bank of Angola in accordance with the provisions of Article 7 of Aviso Nº 01/2002 (Article 6(1)(d)).

As per Article 5, only authorised institutions, authorised in accordance with the legal and regulatory rules, may provide payment services.

Article 7(2) of Aviso Nº 01/2002 requires non-financial legal persons (firms or corporations) with local majority stake holding (capital) to obtain authorisation from the *Banco Nacional de Angola* for the provision of payment services referred to in paragraph a) of Article 4. Non-financial legal persons (firms or corporations) with local majority stake holding (capital) must have:

- share capital not less than USD 250,000.00 (two hundred fifty thousand U.S. dollars), subscribed and fully paid and deposited in the institution domiciled in the country;
- have the object of their activity as being the provision of payment services;
- make adequate provision for technical and technological infrastructure.

Article 8 sets out the requirements and procedure for applications for authorisation of non-financial legal persons (firms or corporations) with local majority stake holding (capital).

Article 9 sets out safeguarding requirements and requires entities providing payment services referred to in paragraph a) of article 4, except banks and credit unions to maintain the “exclusive transit of funds received for payment to the final beneficiary bank account in the provision of this payment service.”

Article 10 reads, “the *Banco Nacional de Angola* may order the cessation of the provision of payment services by any of the entities referred to in this Notice, when the quality of services not meet the objectives of the Payment System of Angola or verify compliance with rules of its subsystems.”

While the DRC does not have a standalone law covering all of the provisions found in the Payment Services Directive, the DRC has adopted a unique approach and is the only SADC country to combine provisions found in “conventional” National Payment System Acts with several of the consumer protection orientated provisions found in the PSD. The drafters of the DRC’s Draft Law appear however to have been highly selective in terms of which PSD provisions they have incorporated into their draft domestic law. Important provisions such as the definition of payment service providers, payment institutions, capital requirements, own funds, safeguarding requirements, authorisation of payment institutions, information requirements for and single payment transactions have been left out.

Some countries have issued related Directives that cover initial capital requirements for E-Money issuers. It must however be noted that, the scope of these Directives is limited to the subject matter that they cover. The DRC’s Directive No. 24 for example only applies to E-Money issuers. The EU PSD covers the capital requirements for all PSPs (payment institutions). Likewise, Namibia’s (PSD - 3) Determination on Issuing of Electronic Money only covers the initial capital requirements of E-Money issuers and not the full scope as set out in the PSD. The same applies to own funds, safeguarding requirements, authorisation and withdrawal of authorisation.

Angola and Mozambique have issued Aviso's that apply specifically to "Banking Payment Cards." These Aviso's contain some of the transparency conditions and information requirements as set out in the PSD, but the scope of these Aviso's are strictly limited to bank issued cards and not the full range of payment services falling within the scope of the PSD.⁶¹¹

Tanzania has also adopted a similar approach. Tanzania does not have a standalone law covering all of the provisions found in the Payment Services Directive. The country has also not passed a Consumer Protection Act. The Bank of Tanzania has however stated that the draft National Payment System Bill contains several consumer protection provisions which cannot be assessed in terms of scope and content at this time. Tanzania's Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania covers several of the transparency conditions and information requirements and sets out the rights and obligations of E-Money issuers, acquirers, merchants and customers. The Tanzanian Guidelines however only apply to bank issued, card based E-Money products.

While Malawi does not have a standalone law covering all of the provisions found in the Payment Services Directive, several important provisions are found in the Malawian Consumer Protection Act, 2003,⁶¹² the Payment Systems Bill, 2014 and the Guidelines for Mobile Payment Systems, 2011. It is important to note however that the Guidelines for Mobile Payment Systems, 2011 applies only to mobile financial payment services. Malawi's Consumer Protection Act, 2003⁶¹³ does not cover the specifics as set out in the PSD. The consumer Protection Act does however contain provisions on standard form contracts (section 26), relief against unfair consumer contracts (section 27), contracts governing financial transactions (section 28), the right of retraction (section 30), implied contractual terms (section 31), cancellation and variation of contracts (section 32), consumer information on standards (section 35), the requirement for the price to be displayed (this also refers to services) (section 36), and measures for consumer redress and mechanisms (Part VIII).

Mauritius does not have a standalone Payment Services Law. Several issues covered in the EU's PSD are however covered in the Bank of Mauritius Guideline on Mobile Banking and Mobile Payment Systems, 2013. It is important to note that the Guideline is limited in scope to Mobile Banking and Mobile Payment Systems and does not cover any of the other payment services as listed in the PSD.

South Africa also does not have a standalone Payment Services Law. Several relevant provisions are however found in the Code of Banking Practice which is a voluntary code code that sets out the minimum standards for service and conduct that consumers can expect from their banks with regard to the services and products the bank offers. The Code only applies to personal and small business customers. This Code contains a number of provisions of general application, and is by its nature, not legally enforceable.

Tables 57 to 59 below map the provisions found in the PSD against relevant provision in domestic law and regulations of each SADC Member State.

⁶¹¹ Article 2 of Mozambique's Aviso n° 1/GBM/2014 of 4 June reads, "this Regulation applies to credit institutions and financial companies authorised to issue bank cards, in accordance with applicable law, as well as to the owners and users of these cards." Similarly, Angola's Notice No. 09/2011 of 13 October – Rules of Banking Payment Cards applies only to the activities of issuance, acceptance and use of payment cards.

⁶¹² Act 14 of 2003.

⁶¹³ Act 14 of 2003.

Table 57: Provisions on Payment Services

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW
Payment service provider defined in law or regulation	x	x	x	x	x	x	✓	✓ ⁶¹⁴	x	✓ ⁶¹⁵	x	x	✓ ⁶¹⁶	x
Payment services are defined	✓ ⁶¹⁷	x	x	x	x	x	✓ ⁶¹⁸	✓ ⁶¹⁹	x	● ⁶²⁰	x	x	x	x
Payment institution defined	✓ ⁶²¹	x	x	x	x	x	x	x	x	● ⁶²²	x	x	x	x
Application for authorisation as a payment institution	✓ ⁶²³	x	x	x	● ⁶²⁴	x	x	x	x	x	x	x	✓ ⁶²⁵	x

⁶¹⁴ Section 1 Payment System Management Act, 2003 (As Amended). Service provider is defined as a person registered as contemplated in section 3(6)(a) as service provider. Section 3(6)(a) reads, "The Body must register a person who is not a system participant as service provider and authorise such persons to provide one or more payment system services, if that person meets the requirements and conditions set out in the Body's rules." The Namibian definition is much narrower than the definition contained in the PSD. The PSD definition includes inter alia: credit institutions (banks), e-money institutions, post office giro institutions, payment institutions, Central Banks.

⁶¹⁵ Directive No. 1 of 2007. "Payer service provider" is defined as, "a person who accepts money or the proceeds of payment instructions, as a regular feature of that person's business, from a payer to make payment on behalf of that payer to multiple beneficiaries."

⁶¹⁶ Section 12 National Payment Systems Act 1 of 2007. This is of narrow application as payment system businesses are narrowly defined.

⁶¹⁷ Articles 3 and 4 Aviso N° 01/2002.

⁶¹⁸ See the definition of "Payment Service Provider" and "Service charge" respectively in the Glossary of Law n° 2/2008, of 27 February.

⁶¹⁹ Section 1 Payment System Management Act, 2003 (As Amended).

⁶²⁰ Position Paper 02/2007. Payment services are defined in paragraph 5.1 of Position Paper 02/2007 Bank Models in the National Payment System as, "being the services whereby a bank enables its clients to (a) make third-party payments by providing its clients with the means to issue payments to the clients of another bank or the other bank itself, through direct access to their (the bank's clients') bank accounts; (b) receive payments directly into their (the bank's clients') accounts from clients of another bank or the other bank itself; (c) withdraw cash at another bank." Paragraph 5.2 lists a number of ways in which clearing banks usually provide payment services to their clients. These include: issuing paper-based debit pull instruments (cheques books in the clients own name, facilities to allow clients of another bank to withdraw funds electronically from their accounts); issuing card based debit-pull instruments with itself (the bank) designated as the payment bank (credit cards, debit cards, fleet cards); providing the collection facilities for debit-pull payment instructions such as cheques, debit orders, ATM withdrawals, PoS initiated transactions; providing facilities to pay away an or receive funds through credit push payments such as credit orders, stop orders and salary payments.

⁶²¹ Article 6 Aviso N° 01/2002.

⁶²² Position Paper 02/2007. Payment services are limited to services provided by clearing banks.

⁶²³ Article 8 Aviso N° 01/2002.

Initial capital requirements for PSPs	✓	✗	✓ 626	✗	● ⁶²⁷	✗	✗	✓ 628	✗	✗	✗	✗	✗	✗
Own funds	✗	✗	✓ 629	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Safeguarding requirements	✓ 630	✗	✓ 631	✗	✗	✗	✗	✓ 632	● ⁶³³	✗	✗	✗	✗	✗
Granting of authorisation	✓ 634	✗	✓ 635	✗	●	✗	● ⁶³⁶	✓ 637	● ⁶³⁹	✗	✗	● ⁶⁴⁰	✗	✗

⁶²⁴ See section 12(1) Payment Systems Bill and the Guidelines on Mobile Payments Systems. Although payment institutions are not defined in the PSB, no person may establish or operate any payment, clearing and settlement system or service including electronic money transfer, remittance services or issue payment instruments without prior authorisation from the Reserve Bank of Malawi.

⁶²⁵ Narrow application – application for designation as a payment system business.

⁶²⁶ Directive No. 24. This Directive however only applies to e-money issuers. The EU PSD covers the capital requirements for all PSPs (payment institutions).

⁶²⁷ Section 13(4) Payment Systems Bill. The Reserve Bank of Malawi may stipulate more detailed requirements regarding activities, legal form, fit and proper management, capital, risk management and security requirements.

⁶²⁸ (PSD - 3) Determination on Issuing of Electronic Money. The Namibian PSD-3 only covers the initial capital requirements of e-money issuers. The EU PSD covers capital requirements for all PSPs.

⁶²⁹ Directive No. 24. This only applies to e-money issuers. The EU PSD covers own fund requirements for all PSPs (payment institutions).

⁶³⁰ Article 9 Aviso N° 01/2002.

⁶³¹ Directive No. 24. This only applies to e-money issuers. The EU PSD covers own fund requirements for all PSPs (payment institutions).

⁶³² (PSD - 3) Determination on Issuing of Electronic Money. The Namibian PSD-3 only covers safeguarding requirements for e-money issuers. The EU PSD covers all PSPs including credit institutions.

⁶³³ Draft Directive on Mobile Payment Services. This applies to mobile money issuers and service providers only.

⁶³⁴ Article 7(2) Aviso N° 01/2002.

⁶³⁵ Directive No. 24. This only applies to e-money issuers.

⁶³⁶ Bank of Mauritius Guideline on Mobile Banking and Mobile Payment Systems, 2013. This only applies to mobile products offered by both banks and non-banks.

⁶³⁷ (PSD - 3) Determination on Issuing of Electronic Money. PSD-3 only applies to e-money issuers.

⁶³⁸ (PSD - 1) Determination on Issuing of a Payment Instrument in Namibia (PSD-1), issued on 29 June 2007. Section 2 reads, “this determination shall apply to all persons who intend to issue a payment instrument in Namibia in terms of section 5 of the Payment System Management Act, 2003 (Act No. 18 of 2003). Payment system participants as defined in the Payment System Management Act shall only seek authorization for issuing e-money or similar new payment instrument. Current payment instrument issuers shall be subjected to an assessment process, based on this determination, in order to ensure compliance with minimum requirements for issuing payment instruments in Namibia.”

⁶³⁹ Draft Directive on Mobile Payment Services. This applies to mobile money issuers and service providers only.

⁶⁴⁰ Paragraph 9(1) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania requires the Bank of Tanzania through its Directorate of National Payment System to authorise the introduction and operation of auditable E-Money products and schemes in Tanzania subject to the adherence of several non-negotiable criteria. If compared against Article 10 of the PSD that requires Member States to require a payment institution that intends to provide payment services to obtain

Withdrawal of authorisation	✓ 641	✗	✓ 642	✗	● ⁶⁴³	✗	● ⁶⁴⁴	✓ 645 ✓ 646	● ⁶⁴⁷	✗	✗	✗	✗	✗
Public register of authorised payment institutions, their agents and branches	✗	✗	✗	✗	✗	✗	✗	✗ 648	✗	✗	✗	✗	✗	✗
Statutory audit	✗	✗	✗	✗	✗	✗	✗	✗	● ⁶⁴⁹	✗	✗	● ⁶⁵⁰	✗	✗
Use of agents, branches or entities to which activities are outsourced	✗	✗	✓ 651	✗	●	● ⁶⁵²	✓ 653	✓ 654	✗	✗	✗	✗	✗	✗
PSP remain liable for acts of employees, agents and branches	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Designation of Competent Authorities	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Supervision of PSPs Professional secrecy	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Right to apply to court	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓ ⁶⁵⁵	✗

authorisation as a payment institution before commencing the provision of payment services, the Tanzanian provision is very limited in scope due to the technology specific nature of the Guideline.

⁶⁴¹ Article 10 Aviso N° 01/2002.

⁶⁴² Directive No. 24. This only applies to e-money issuers.

⁶⁴³ Section 17 Payments Systems Bill.

⁶⁴⁴ Bank of Mauritius Guideline on Mobile Banking and Mobile Payment Systems, 2013. This only applies to mobile products offered by both banks and non-banks.

⁶⁴⁵ (PSD - 3) Determination on Issuing of Electronic Money. PSD-3 only applies to e-money issuers.

⁶⁴⁶ Section 9 and 10 (PSD - 1) Determination on Issuing of a Payment Instrument in Namibia (PSD-1), issued on 29 June 2007.

⁶⁴⁷ Draft Directive on Mobile Payment Services. This applies to mobile money issuers and service providers only.

⁶⁴⁸ The EU PSD requires Member States to establish a public register of authorised payment institutions, their agents and branches, as well as of natural and legal persons, their agents and branches.

⁶⁴⁹ Draft Directive on Mobile Payment Services. This applies to an audit during the pilot phase only.

⁶⁵⁰ The Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania requires that E-Money products and schemes should provide an accurate and fully accessible audit trail of transactions from the originator of payment to its finality. The Guidelines do not however contain a specific requirement that E-Money issuers must have their annual reports audited by statutory auditors or audit firms.

⁶⁵¹ Directive No. 24. This only applies to e-money issuers.

⁶⁵² See Guideline on Mobile Banking and Mobile Payment Systems. This only applies to mobile products offered by both banks and non-banks.

⁶⁵³ See Decree 30/3014 of 5 June that amends the Regulation Law of Credit Institutions and Financial Companies, approved by Decree 56/2004 of 10 December.

⁶⁵⁴ (PSD - 3) Determination on Issuing of Electronic Money. PSD-3 only applies to e-money issuers.

⁶⁵⁵ Section 12(6) National Payment Systems Act, 2007.

Exercise of the right of establishment and freedom to provide services in other Member States	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Access to payment systems	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Prohibition for persons other than PSP to provide payment services	x	x	x	x	x	x	x	x	x	x	x	x	✓ ⁶⁵⁶	x

⁶⁵⁶ Sections 12 and 13. Only applies to "Payment System Businesses".

Title II of the PSD covers the transparency of conditions and information requirements for payment services. It includes *inter alia* the prohibition against charging for information, the derogation from information requirements permitted for low-value payment instruments and E-Money, prior general information requirements for single payment transactions, information requirements for the payer after receipt of a payment order, information requirements for the payee after the execution of a single payment transaction, information and conditions for framework contracts, the ruminant of framework contracts and common provisions on currency and conversion. As can be seen in Table 58 below, this is an area that needs addressing in all fourteen SADC Member States.

Table 58: Transparency Conditions and Information Requirements

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW
Prohibition against charging for information Burden of proof on information requirements	x	x	x	x	x	x	x	x	x	● 657	x	x	x	x
Derogation from information requirements for low-value payment instruments and E-Money	x	x	x	x	x	x	x	x	x	✓ 658	x	x	x	x
Single payment transactions - prior general information requirements	x	x	x	x	x	x	x	x	x	● 659	x	x	x	x
Single payment transactions - information and conditions	x	x	x	x	x	x	x	x	x	● 660	x	x	x	x
Single payment transactions - information for the payer after receipt of the payment order	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Single payment transactions - information for the payee after execution	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Framework contracts - prior general information	✓ 661	x	● 662	x	x	x	x	x 663	x	✓ 664 ● 665	x	● 666	x	x

⁶⁵⁷ See section 6.8 of the Code of Banking Practice, 2012.

⁶⁵⁸ Exemption 17, Circular 6 and the Low-Value Prepaid Exemption.

⁶⁵⁹ Section 3.1 of the Code of Banking Practice, 2012 states *inter alia* that, "as a customer or potential customer you can expect the following reasonable conduct from your bank as more fully outlined and detailed in the body of the Code. Your bank will provide you with effective and adequate disclosure of information, including the Terms and Conditions of products and services."

⁶⁶⁰ Section 3.1 of the Code of Banking Practice, 2012.

⁶⁶¹ Article 5(2) Aviso N° 09/2011. This Aviso only applies to "banking payment cards."

⁶⁶² Articles 19, 20 and 45 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁶³ The provision in PSD-3 only applies to contracts with agents and service providers.

⁶⁶⁴ Consumer Protection Act 68 of 2008.

Framework contracts - information and conditions	✓ 667	x	● 668	x	x	x	✓ 669	x	x	✓ 670 ● 671	x	● 672	x	x
Framework contracts - changes in conditions of the framework contract	x	x	● 673	x	x	x	✓ 674	x	x	● 675	x	● 676	x	x
Framework contracts - termination	x	x	x	x	x	x	x	x	x	● 677	x	x	x	x
Framework contracts - information before execution of individual payment transactions	x	x	x	x	x	x	x	x	x	● 678	x	x	x	x

⁶⁶⁵ General provisions are found in the Code of Banking Practice, 2012.

⁶⁶⁶ Paragraph 11(6) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania sets out the information that must be provided to consumers / users of Card Based Electronic Money products.

⁶⁶⁷ Articles 3 and 5 Aviso N° 09/2011. This Aviso only applies to "banking payment cards."

⁶⁶⁸ Article 45 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁶⁹ Articles 4, 5 and 6 Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks. It is specifically provided that the relationship established between the issuer and the user should be regulated through a written contract and also that it may be through an adhesion contract. This contract must outline the general conditions for the use of the cards and can only be altered by means of a written communication with a form of acknowledgement receipt addressed to the card holder with a prior notice of 30 days.

⁶⁷⁰ Consumer Protection Act 68 of 2008.

⁶⁷¹ General provisions are found in the Code of Banking Practice, 2012.

⁶⁷² The Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania contains several provisions on the informations and provisions that must be included in the contract governing the relationship between the issuer of Card Based Electronic Money products and users. Paragraph 11.5(ii) requires parties to enter into a solid and transparent legal agreement that clearly states the rights and obligations of each party. See [section L2.5](#) of Annexure L for additional information on the requirements that must be set out in the contracts applicable to Card Based Electronic Money products in Tanzania.

⁶⁷³ Article 45 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁷⁴ Articles 5(2) Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks.

⁶⁷⁵ Section 3.1 of the Code of Banking Practice, 2012 states *inter alia* that, "your bank will provide you with at least 20 business days (or 5 business days in the case of credit agreements) notice before the implementation of changes in the Terms and Conditions, fees and charges, the discontinuation of products and / or services and the relocation of premises."

⁶⁷⁶ Paragraph 12.5(viii) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania permits issuers to amend terms and conditions of payment card issuance, interest charge changes, renewal criteria, annual fees etc. upon sufficient advance period to payment card participants. No time period is specified.

⁶⁷⁷ General provisions are found in the Code of Banking Practice, 2012.

⁶⁷⁸ General provisions are found in the Code of Banking Practice, 2012.

Framework contracts - information for the payer on individual payment transactions	✓ ⁶⁷⁹	x	x	x	x	x	x	x	x	x	● ⁶⁸⁰	x	● ⁶⁸¹	x	x
Framework contracts - information for the payee on individual payment transactions	x	x	x	x	x	x	x	x	x	x	● ⁶⁸²	x	x	x	x
Common provisions - currency and currency conversion	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Common provisions - information on additional charges or reductions	x	x	● ⁶⁸³	x	x	x	x	x	x	x	● ⁶⁸⁴	x	x	x	x

⁶⁷⁹ Article 4(6) of Aviso N° 09/2011 requires that account statements and other information to holders must show, a) fees and other charges that apply, taxes (if applicable) on a per transaction basis, b) the identification of foreign currency, the value of transactions in that currency and its equivalence to Kwanza. Aviso N° 09/2011 only applies to “bank card payments.”

⁶⁸⁰ General provisions are found in the Code of Banking Practice, 2012.

⁶⁸¹ Paragraph 11.6(viii) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania requires that consumers be provided with duly authenticated records of transactions and a statement of account, minimally on a monthly basis.

⁶⁸² General provisions are found in the Code of Banking Practice, 2012.

⁶⁸³ Article 20 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁸ General provisions are found in the Code of Banking Practice, 2012.

Title IV covers rights and obligations in relation to the provision and use of payment services (payment instruments). Important issues covered include the authorisation of payment transactions, consent and withdrawal of consent, obligations of payment service providers in relation to payment instruments, notification of unauthorised or incorrectly executed payment transactions, payer's liability for unauthorised payment transactions, refunds, refusal of payment orders, execution time and value date, cash placed on a payment account, right of recourse, data protection and complaints procedures. As indicated in Table 59 below, this is also an area that needs addressing in all fourteen SADC Member States.

Table 59: Rights and Obligations in Relation to the Provision of Payment Services

	ANG	BWA	DRC	LSO	MW	MU	MZ	NA	SC	RSA	SW	TZ	ZM	ZW
Charges Applicable	x	x	● ⁶⁸⁵	x	x	x	x	x	x	x	x	x	x	x
Derogation for low value payment instruments and E-Money	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Authorisation of payment transactions - consent and withdrawal of consent	x	x	✓ 686	x	x	x	x	x	x	x	x	x	x	x
Authorisation of payment transactions - limits of the use of payment instruments	x	x	x	x	x	● ⁶⁸⁷	x	✓ 688	x	x	x	● ⁶⁸⁹	x	x
Obligations of the payment service user in relation to payment instruments	x	x	● ⁶⁹⁰	x	x	x	✓ 691	x	x	● ⁶⁹²	x	● ⁶⁹³	x	x
Obligations of the payment service provider in relation to	x	x	● ⁶⁹⁴	x	x	x	✓ 695	x	x	● ⁶⁹⁶	x	● ⁶⁹⁷	x	x

⁶⁸⁵ Article 20 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁸⁶ Inferred.

⁶⁸⁷ Guideline on Mobile Banking and Mobile Payment Systems. This only applies to mobile products offered by both banks and non-banks.

⁶⁸⁸ (PSD - 3) Determination on Issuing of Electronic Money. PSD-3 only applies to e-money transaction limits.

⁶⁸⁹ Paragraph 12.5(vi) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania permits issuers to independently set an interest rate, fees and charges related to the use of a payment card. Paragraph 12.4(iii) requires the issuer to execute a payment instruction issued by the customer unless inadequate funds are available, the payment instruction is incomplete, the payment instruction is attached with a notice or the issuer has reason to believe that the payment instruction is issued to carry out an unlawful transaction.

⁶⁹⁰ Articles 51 to 55 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁹¹ Several provisions are found in Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks and the users thereof.

⁶⁹² Section 3.2 of the Code of Banking Practice, 2012.

⁶⁹³ Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania contains several provisions on the obligations of the users of card based E-Money products.

⁶⁹⁴ Article 51 to 55 Proposed Draft Law on Provisions Applicable to the National Payment System.

payment instruments															
Notification of unauthorised or incorrectly executed payment transactions	x	x	● 698	x	x	x	✓ 699	x	x	● 700	x	x	x	x	
Evidence on authentication and execution of payment transactions	x	x	x	x	x	x	x	x	x	● 701	x	x	x	x	
PSPs liability for unauthorised payment transactions	✓ 702	x	● 703	x	x	x	x	x	x	● 704	x	x	x	x	
Payer's liability for unauthorised transactions	✓ 705	x	● 706	x	x	x	x	x	x	● 707	x	x	x	x	
Refund of payment transactions initiated by or through a payee	x	x	x	x	x	x	x	x	x	*708	x	x	x	x	
Requests for refunds for payment transactions initiated by or through a payee	x	x	x	x	x	x	x	x	x	*709	x	x	x	x	
Payment orders and amounts transferred - receipt of payment orders	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Refusal of payment orders	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Irrevocability of a payment order by a Payment Service User	x	x	● 710	x	x	x	x	x	x	x	x	x	x	x	

⁶⁹⁵ Several provisions are found in Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks and the users thereof.

⁶⁹⁶ General provisions are found in the Code of Banking Practice, 2012.

⁶⁹⁷ Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania contains several provisions on the obligations of the issuers of E-Money products.

⁶⁹⁸ Article 55 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁶⁹⁹ Article 10 Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks and the users thereof.

⁷⁰⁰ General provisions are found in the Code of Banking Practice, 2012.

⁷⁰¹ General provisions are found in the Code of Banking Practice, 2012.

⁷⁰² Article 5 Aviso N° 09/2011. This Aviso only applies to "banking payment cards."

⁷⁰³ Article 25 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁷⁰⁴ General provisions are found in the Code of Banking Practice, 2012.

⁷⁰⁵ Article 5 Aviso N° 09/2011. This Aviso only applies to "banking payment cards."

⁷⁰⁶ Article 27 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁷⁰⁷ General provisions are found in Section 3.2 of the Code of Banking Practice, 2012.

⁷⁰⁸ See PASA Rules.

⁷⁰⁹ See PASA Rules on return of funds, procedures and processes.

⁷¹⁰ Article 35 Proposed Draft Law on Provisions Applicable to the National Payment System.

Amounts transferred and amounts received	x	x	● 711	x	x	x	x	x	x	x	x	x	x	x
Execution time and value date	x	x	● 712	x	x	x	✓ 713	x	x	x	x	● 714	x	x
Payment transactions to a payment account	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Cash placed on a payment account	x	x	x	x	x	x	x	x	x	x	x	x	x	x
National payment transactions	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Value date and availability of funds	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Liability - incorrect unique identifiers	x	x	x	x	x	x	✓ 715	x	x	x	x	x	x	x
Liability - non-execution or defective execution	x	x	x	x	x	x	✓	x	x	x	x	● 716	x	x
Right of recourse	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Data protection	x	x	x	x	x	x	x	x	x	● 717	x	x	x	x
Complaint procedures	x	✓ 718	x	x	✓ 719	● 720	✓ 721	x	● 722	✓ 723	x	x	x	x
										● 724				

⁷¹¹ Article 37 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁷¹² Article 36 Proposed Draft Law on Provisions Applicable to the National Payment System.

⁷¹³ See Article 13(3) of Law n° 2/2008, of 27 February.

⁷¹⁴ Paragraph 9(1) of the Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania requires Acquirers to execute the payment instruction on the payment card scheme working day on which the payment instruction is received.

⁷¹⁵ See Article 17 of Regulation Subsystem Interbank Clearing and Settlement approved by Aviso n° 17/2013, of 31 December.

⁷¹⁶ The Tanzanian Guidelines on the Operation of Auditable Card Based Electronic Money Schemes in Tanzania contains several provisions on liability. For example, paragraph 11.5(ii)(k) reads, "in the event of any delay in the completion of the funds transfer or any loss due to an error in the execution of the funds transfer pursuant to a payment instruction, the Issuer's liability shall be limited to the extent of payment of interest at the bank rate for any period of delay in the case of delayed payment and refund of the amount together with interest at the Issuer rate up to the date of refund, in the event of loss due to an error, negligence or fraud on the part of the Issuer."

⁷¹⁷ General provisions are found in section 3.1 and 6 of the Code of Banking Practice, 2012.

⁷¹⁸ S7 Consumer Protection Act [Chapter 42:07].

⁷¹⁹ Part VIII Consumer Protection Act 14 of 2003.

⁷²⁰ Guideline on Mobile Banking and Mobile Payment Systems. The Guideline contains a comprehensive complaints mechanism. This only applies however to mobile products offered by both bank and non-banks.

⁷²¹ Complaint procedures are set out in Aviso n° 4/4009, of March 4 - Regulation of Care Services Complaints, Enquiries and Suggestions.

⁷²² Consumer Protection Act. This is a general provision and mechanism only.

⁷²³ Consumer Protection Act 68 of 2008.

Penalties	x	x	x	x	x	x	✓ 725	x	x	x	x	x	x	x
							✓ 726							
Complaints procedure to be administered by Competent Authorities	x	x	x	x	✓ 727	x	x	x	x	x	x	x	x	x
Out of Court redress	x	x	x	x	x	x	✓ 728	x	x	✓ 729	x	x	x	x
										● 730				

⁷²⁴ General provisions are found in the Code of Banking Practice, 2012. Section 10 covers dispute resolution and the Ombudsman for Banking Services.

⁷²⁵ A general provision on penalties is found in Law n° 2/2008, of 27 February.

⁷²⁶ See Article 24 Aviso n° 1/GBM/2014 of 4 June Regulations of Bank Cards. This applies only to cards issued by banks.

⁷²⁷ Part VIII Consumer Protection Act, 2003.

⁷²⁸ See the general provision, Article 34 in Law n° 2/2008, of 27 February.

⁷²⁹ Consumer Protection Act 68 of 2008 / Banking Adjudicator.

⁷³⁰ General provisions are found in the Code of Banking Practice, 2012. Section 10 covers dispute resolution and the Ombudsman for Banking Services.

SECTION 9: ANTI-MONEY LAUNDERING

Anti-money laundering and counter terrorist financing requirements and regulatory measures are becoming increasingly important to regulators tasked with ensuring the safety, efficiency and security of payment systems, products and distribution channels. The importance of a harmonised AML regulatory framework for SADC is set out in Annex 12 of the SADC Protocol of Finance and Investment. The preamble to Annex 12 states that, "harmonisation of key aspects of relevant laws and policies will increase the effectiveness of the measures taken by State Parties to address money laundering and financing of terrorism in the region and support finance and investment." Further, that "harmonisation of key aspects of the relevant laws and policies will create an enabling environment for increased access to financial services in the region, minimise compliance costs for affected Regulated Institutions that operate cross-border in the region and lessen the danger that criminal acts will be displaced from one State Party to another. It is important to note that the preamble affirms the importance of the full implementation of the Financial Action Task Force (FATF) Recommendations and that any action undertaken by SADC in this area should be consistent with other actions undertaken in other international forums. Annex 12 of the FIP is legally binding on all signatories. As such, the choice of the FATF Recommendations as the de facto standard for harmonisation of all AML/CFT laws and regulations in the SADC region is mandated.

For the purposes of the review of the Legal and Regulatory Framework for Payments in the SADC Region, seven of the FATF recommendations are particularly relevant to retail payments and serve as a harmonisation benchmark. These are FATF Recommendation 1) Assessing Risks and Applying the Risk Based Approach; Recommendation 10) Customer Due Diligence; Recommendation 11) Record Keeping; Recommendation 13) Correspondent Banking; Recommendation 15) New Technologies; Recommendation 16: Wire Transfers and Recommendation 17) Reliance on Third Parties. The section that follows benchmarks the provisions found in each SADC Member States AML laws and regulations against these FATF Recommendations.

9.1 Level of Compliance with Recommendation 10: CDD

9.1.1 Component A: When is CDD Required?

[FATF Recommendation 10](#) contains essential components applicable to the CDD requirements for 'standard' customer relationships and transactions. These are Component A) the description of when CDD is required; Component B) identification measures and acceptable verification sources; and Component C) the timing and verification of identity. In the section that follows, each of these components is reviewed individually. While these three components apply to 'standard' customer relationships and transactions, the FATF Recommendations require the application of the risk based approach to CDD, allowing countries to permit financial institutions to apply simplified measures where there is a lower risk of money laundering and terrorist financing and in some cases to apply the Proven Low Risk Exemption or the De Minimis Exemption. As such, this section also examines each countries approach to simplified measures and various exemptions contained in law and regulation.

Section 15 of the recently enacted Zimbabwean Money Laundering and Proceeds of Crime Act, 2013⁷³¹ is the most compliant provision found in a statute in the SADC region with respect to component (1) of FATF Recommendation 10. Section 15 of the Money Laundering and Proceeds of Crime Act, 2013 requires every financial institution and designated non-financial business or profession to identify each one of its customers and verify a customer's identity by means of an identity document when:

- opening an account for or otherwise establishing a business relationship with a customer;⁷³²
- when the customer, who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out a transaction in an amount equal to or exceeding five thousand United States dollars USD 5,000 (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution), whether conducted as a single transaction or several transactions that appear to be linked, provided that the amount of the transaction is unknown at the time it is commenced, the customer's identification shall be verified as soon as the amount of the transaction has reached the prescribed amount;⁷³³
- when the customer, whether or not he or she is in an established business relationship with the financial institution, wishes to carry out a domestic or international wire transfer or monetary amounts in the amount equal to or exceeding one thousand United States dollars (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution);⁷³⁴
- where doubt exists regarding the veracity or adequacy of previously obtained identity documents⁷³⁵ or
- where there is a suspicion of money laundering or financing of terrorism involving the customer or the customer's account.⁷³⁶

Section 15(1) of the Zimbabwean Money Laundering and Proceeds of Crime Act, 2013 contains all 5 key requirements listed for when CDD is required and, as a "new generation" Act, (passed after the new FATF Recommendations were published in 2012), contains an exemption for domestic and international wire transfers less than USD1, 000 as suggested in the FATF Interpretive Note 16, paragraph 5. It is however important to note that FATF still requires financial institutions to include accurate originator information and a unique account number or reference number in cross-border wire transfers, but stipulates that this information need not be verified for accuracy for transfers less than USD1,000. The Zimbabwean threshold of USD5, 000 set out in section 15(1)(b) of the Money Laundering and Proceeds of Crime Act, 2013 for an occasional transaction is still well below the threshold of USD 15, 000 recommended by FATF.

⁷³¹ Act 4 of 2013.

⁷³² Section 15(1)(a) Act 4 of 2013.

⁷³³ Section 15(1)(b).

⁷³⁴ Section 15(1)(c).

⁷³⁵ Section 15(1)(d).

⁷³⁶ Section 15(1)(e).

As depicted in Table 60 below, all fourteen countries require financial institutions to conduct CDD when establishing a business relationship and conducting an occasional transaction. The provision on occasional transactions in either the law or regulation in several countries does not set a threshold. This is the case in Botswana, Namibia, South Africa, Tanzania and Zambia.

Table 6o: Compliance with Component A FATF Recommendation 1o: When is CDD required?

Country	A CDD required when establishing a business relationship	B CDD required when conducting an occasional transaction	C CDD not required when conducting an occasional transaction below a set threshold (Proven Low Risk Exemption)	D CDD required when carrying out an occasional transfers that is a wire transfers	E CDD not required when carrying out an occasional transfer that is a wire transfer below the USD1,000 threshold (Proven Low Risk Exemption)	F CDD always required when there is a suspicion of ML/TF	G CDD required when Financial institution has doubts about the veracity or adequacy of previously obtained customer identification data	H Anonymous accounts are prohibited
Angola See Annexure A, section A2.7.3.1	✓ Article 5(1)(a) Law n° 34/11	✓ Article 5(1)(b) Law n° 34/11	✓ Article 5(1)(b) Law n° 34/11	✗	✗	✓ Article 5(1)(c) Law n° 34/11	✓ Article 5(1)(d) Law n° 34/11	✓ Article 21(2) Law n° 34/11
Botswana See Annexure B, section B2.7.3.1	✓ S 10(1)(a) Financial Intelligence Agency Act, 2009; ⁷³⁷ S16A(5) Proceeds of Serious Crime Act, 1990 ⁷³⁸	✓ Section 10(1)(a) Financial Intelligence Agency Act, 2009; 16A (5) Proceeds of Serious Crime Act, 1990	✗	✗	✗	✓ S16A(5) Proceeds of Serious Crime Act, 1990	✗	✓ ⁷³⁹ Regulation 10 Banking (Anti-Money Laundering) Regulations, 2003

⁷³⁷ Act 6 of 2009.

⁷³⁸ Act 19 of 1990.

⁷³⁹ Anonymous accounts are not prohibited in the Financial Intelligence Agency Act 6 of 2009 or the Proceeds of Serious Crime Act, 1990 (As Amended). Regulation 10 of the Banking (Anti-Money Laundering) Regulations, 2003 however specifically prohibits banks from opening or keeping anonymous accounts or accounts in obviously fictitious

DRC See Annexure C, section C2.7.3.1	✓ Article 8 of Law n° 04/016	✓ Article 9 of Law n° 04/016	✓ Article 9 of Law n° 04/016	✗	✗	✓ Article 9 of Law n° 04/016	✗	✗
Lesotho See Annexure D, section D2.7.3.1	✓ S16(1) Money Laundering and Proceeds of Crime Act, 2008 ⁷⁴⁰	✓ ⁷⁴¹ S16 Money Laundering and Proceeds of Crime Act, 2008	✓ S 16(9)(d) Money Laundering and Proceeds of Crime Act, 2008	✓ ⁷⁴² : S16(2)(a) Money Laundering and Proceeds of Crime Act, 2008	✗	✓ S16(2)(b) Money Laundering and Proceeds of Crime Act, 2008	✓ S 16(2)(c) Money Laundering and Proceeds of Crime Act, 2008	✓ S 17(2) and S 26 of the Money Laundering and Proceeds of Crime Act, 2008
Malawi See Annexure E, section E2.7.3.1	✓ S24(1) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006; ⁷⁴³	✓ ⁷⁴⁴ Regulation 3(1) of the Money Laundering, Proceeds of Serious Crime	✓ Regulation 3(1)(b) Money Laundering, Proceeds of Serious Crime and Terrorist Financing	✓ ⁷⁴⁵ Regulation 3(1)(b) Money Laundering, Proceeds of Serious Crime and Terrorist	✗	✓ Regulation 3(1)(e) Money Laundering, Proceeds of Serious Crime and Terrorist Financing	✓ Regulation 3(1)(f) Money Laundering, Proceeds of Serious Crime and Terrorist Financing	✓ Regulation 3(2) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing

names. The Financial Intelligence Agency Act 6 of 2009 does not contain explicit provisions prohibiting the opening of fictitious accounts, however, section 10(4) makes it an offence for a person to transact with a specified party using false documents.

⁷⁴⁰ Act 4 of 2008.

⁷⁴¹ The threshold approach is introduced in section 16(4) of Lesotho's Money Laundering and Proceeds of Crime Act, 2008, but instead of referring to "occasional transactions above USD 15,000" as is required by FATF Recommendation 10, the provision requires accountable institutions to take reasonable measures to ascertain the purpose of **any** transaction in excess of M100, 000 or any amount as may be prescribed by the Minister by notice published in the Gazette and to establish the origin and ultimate destination of the funds involved. This section is supported by section 16(9)(d) that provides and exemption for occasional transactions below M100, 000 and reads, "nothing in this section shall require the production of any evidence of identity where the transaction is an occasional transaction not exceeding M100,000 or any amount as may be prescribed by the Minister by notice in a Gazette, unless the accountable institution has reason to suspect that the transaction is suspicious or unusual."

⁷⁴² Although s16(2)(a) of the Money Laundering and Proceeds of Crime Act, 2008 requires accountable institutions to perform customer verification where a customer is carrying out an electronic transfer, the provision does not specifically address "occasional wire transfer transactions".

⁷⁴³ Act 11 of 2006.

	Regulation 3(1)(a) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	and Terrorist Financing Regulations, 2011	Regulations, 2011	Financing Regulations, 2011		Regulations, 2011	Regulations, 2011	Regulations, 2011
Mauritius See Annexure F, section F2.7.3.1	✓ S17 Financial Intelligence and Anti-Money Laundering Act, 2002; ⁷⁴⁶ Regulation 4(2)(a) Financial Intelligence and Anti-Money Laundering Regulations	✓ ⁷⁴⁷ Regulation 4(2)(b) Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓ Regulation 4(2)(c) Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✗	✗	✗ ⁷⁴⁸ Regulation 4(b) Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✗	✓ Regulation 3(1) Financial Intelligence and Anti-Money Laundering Regulation, 2003 (As Amended)

⁷⁴⁴ It is important to note that section 24(1)(a)(ii) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 which reads “every financial institution shall, before entering into a business relationship with a customer, ascertain the identity of the customer or beneficial owner on the basis of an official or other identifying document, and shall verify the identity of the customer on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer when – (a) a financial institution – (ii) in the absence of a business relationship, conducts any transaction” does not set a threshold to the transaction or mention that it is an “occasional transaction”. This deficiency is however resolved by Regulation 3(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.

⁷⁴⁵ Regulation 3(1)(d) also refers to “electronic funds transfer” instead of “wire transfer”. However, in the context of carrying out CDD, it is accepted that the two descriptions have the same meaning. This regulation does not refer to an “occasional” electronic transfer and therefore applies to all electronic funds transfers.

⁷⁴⁶ Act 6 of 2002.

⁷⁴⁷ Regulation 4(2)(b) requires CDD measures to be undertaken when, “in respect of a one-off transaction, where a relevant person dealing with the transaction knows or has reasonable grounds to suspect that the transaction is a suspicious transaction.”

⁷⁴⁸ The AML Regulations are partially compliant with the FATF Recommendation in this regard as Regulation 4(b) requires CDD measures “in respect of a once-off transaction, where a relevant person dealing with the transaction knows or has reasonable grounds to suspect that the transaction is a suspicious transaction.” Law or regulation does not cover the undertaking of CDD where there is a suspicion of money laundering in connection with a transaction undertaken in the normal course of business.

	2003 (As Amended)							
Mozambique See Annexure G, section G2.7.3.1	✓ Article 10(1)(a) Law n° 14/2013	✓ ⁷⁴⁹ Article 10(1)(b)(i) and (ii) Law n° 14/2013	✓ Article 10(1)(b)(i) and (ii) Law n° 14/2013	✓ Article 10(1)(b)(i) and (ii) Law n° 14/2013	✓ ⁷⁵⁰ Article 10(1)(b)(i) and (ii) Law n° 14/2013	✓ Article 10(1)(c) Law n° 14/2013	✓ Article 10(1)(d) Law n° 14/2013	✓ ⁷⁵¹ Article 10(2)(i) Law n° 14/2013
Namibia See Annexure H, section H2.7.3.1	✓ S21(2)(a) of the Financial Intelligence Act, 2012 ⁷⁵²	✓ S21(2)(a) of the Financial Intelligence Act, 2012	✓ Paragraph 2(1) Exemption Order No. 75: General Exemptions: Financial Intelligence Act, 2007 read together with paragraph 8(3) of Determination FICD 3	✗	✗	✓ S21(2)(d) Financial Intelligence Act, 2012	✗ ⁷⁵³	✓ Section 21(4) Financial Intelligence Act, 2012
Seychelles See Annexure I, section	✓ S4 Anti-Money Laundering Act,	✓ ⁷⁵⁵ S4 Anti-Money	✓ Regulation 8(1)(b) Anti-	✗	✗	✓ Regulation 8(1)(d) Anti-	✓ Regulation 8(1)(c) Anti-	✓ S 7 and S59 Act 5 of 2006 (As

⁷⁴⁹ Article 10(1)(b)(i) of Law n° 14/2013 requires financial institutions and non-financial bodies to identify their customers and confirm their identity through the presentation of valid documents every time they, "effect occasional transactions of amounts equal to or above four hundred and fifty thousand meticaais (i) when the total amount of the transaction is not known at the time of commencement of the operation, the financial entity must proceed with the identification as soon as the amount is known and verify if the threshold has been reached and (ii) in case of a domestic or international transfer."

⁷⁵⁰ It appears from the wording of Article 10(1)(b)(i) of Law n° 14/2013 that the threshold has been set at four hundred and fifty thousand meticaais.

⁷⁵¹ Article 10(2)(i) of Law n° 14/2013 requires financial institutions and non-financial bodies to "avoid" maintaining anonymous accounts or accounts with clearly fictitious identification data. As FATF Recommendation 10 does not allow financial institutions to keep anonymous accounts or accounts in obviously fictitious names, it is suggested that the word "avoid" should be replaced with the words "may not".

⁷⁵² Act 13 of 2012.

⁷⁵³ Contained in Guidance Note 2.

l2.7.3.1	2006 (As Amended); ⁷⁵⁴ Regulation 8(1)(a) Anti-Money Laundering Regulations, 2012	Laundering Act, 2006 (As Amended); Regulation 5 and 8(1)(b) Anti-Money Laundering Regulations, 2012	Money Laundering Regulations, 2012			Money Laundering Regulations, 2012	Money Laundering Regulations, 2012	Amended)
RSA See Annexure J, section J2.7.3.1	✓ ⁷⁵⁶ S21(1) Financial Intelligence Centre Act, 2001 (As Amended) ⁷⁵⁷	✓ S21(1) Financial Intelligence Centre Act, 2001 (As Amended)	✓ ⁷⁵⁸ Various Exemptions	✗	✗	✗	✗	✓ Regulation 2 Money Laundering and Terrorist Financing Control Regulations 2002 (As Amended)
Swaziland See Annexure K, section K2.7.3.1	✓ S6(1)(a)(i) Money Laundering and	✓ S6(1)(a)(ii) Money Laundering	✓ S7 Money Laundering and Financing of	✓ S6(1)(b) Money Laundering and Financing of	✗	✓ S6(1)(c) Money Laundering and Financing of	✓ S6(1)(d) Money Laundering and Financing of	✓ S9(1) Money Laundering and Financing of

⁷⁵⁵ Regulation 5 of the Anti-Money Laundering Regulations, 2012 defines a “once-off-transaction” as a transaction carried out other than as part of a business relationship that exceeds SCR100,000 or SCR50,000 in the case of cash transactions, whether the transaction is carried out in a single operation or several operations which appear to be linked.” SCR100,000 is equivalent to USD 8277.68 and SCR50,000 to USD 4138.84 which are both well, below the threshold suggested by FATF.

⁷⁵⁴ Act 5 of 2006.

⁷⁵⁶ Section 21(1) of the Financial Intelligence Centre Act, 2001 (As Amended) prohibits accountable institutions from establishing a business relationship or concluding a single transaction with a client unless the accountable institution has taken the prescribed steps to: establish and verify the identity of the client; if the client is acting on behalf of another person, to establish and verify the identity of that other person and the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and if another person is acting on behalf of the client, to establish and verify (i) the identity of that other person; and (ii) that other person's authority to act on behalf of the client.

⁷⁵⁷ Act 38 of 2001 (As Amended).

⁷⁵⁸ Several different thresholds are set out in various Exemptions to the Financial Intelligence Act, 2001 (As Amended). These thresholds are determined by the type of product detailed in the exemptions.

	Financing of Terrorism (Prevention) Act 2011	and Financing of Terrorism (Prevention) Act 2011	Terrorism (Prevention) Act 2011	Terrorism (Prevention) Act 2011		Terrorism (Prevention) Act 2011	Terrorism (Prevention) Act 2011	Terrorism (Prevention) Act 2011; S73 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011
Tanzania See Annexure L, section L2.7.3.1	✓ S15(1) of the Anti-Money Laundering Act, 2006 (As Amended); ⁷⁵⁹ Regulation 24(1)(a) Anti-Money Laundering Regulations, 2012	✓ S15(1) of the Anti-Money Laundering Act, 2006 (As Amended); Regulation 24(1)(b) Anti-Money Laundering Regulations, 2012	✗	✗	✗	✓ Regulation 24(1)(c) of the Anti-Money Laundering Regulations, 2012	✓ Regulation 24(1)(d) of the Anti-Money Laundering Regulations, 2012	✓ S19(2) of the Anti-Money Laundering Act, 2006 (As Amended)
Zambia See Annexure M, section M2.7.3.1	✓ S16(1)(a) Financial Intelligence Centre Act, 2010 ⁷⁶⁰	✓ ⁷⁶¹ S16(1)(b) Financial Intelligence Centre Act,	✗	✓ ⁷⁶² S16(1)(c) Financial Intelligence Centre Act, 2010	✗	✓ S16(1)(e) Financial Intelligence Centre Act, 2010	✓ S16(1)(d) Financial Intelligence Centre Act, 2010	✓ S15 Financial Intelligence Centre Act, 2010

⁷⁵⁹ Act 12 of 2006 (As Amended).

⁷⁶⁰ Act 46 of 2010.

⁷⁶¹ Section 16(1)(b) of the) Financial Intelligence Centre Act, 2010 reads, "reporting entities are required to identify and verify their customers' identities by means of reliable and independent source document or information when the customer, who is neither an account holder nor in an established business relationship with a financial institution, wishes to carry out a transaction in an amount equal to, or above, such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked: provided that if the amount of the transaction is unknown, the customer's identification shall be verified as soon as the amount of the transaction has reached the prescribed amount." As far as we have been able to ascertain, the threshold mentioned in sections 16(1)(b) and 16(1)(c) of the Financial Intelligence Centre Act, 2010 have not

		2010						
Zimbabwe	✓	✓	✓	✓	✓	✓	✓	✓
See Annexure N, section N2.7.3.1	S15(1)(a) Money Laundering and Proceeds of Crime Act, 2013 ⁷⁶³	S15(1)(b) Money Laundering and Proceeds of Crime Act, 2013	S15(1)(b) Money Laundering and Proceeds of Crime Act, 2013	S15(1)(c) Money Laundering and Proceeds of Crime Act, 2013	S15(1)(c) Money Laundering and Proceeds of Crime Act, 2013	S15(1)(e) Money Laundering and Proceeds of Crime Act, 2013	S15(1)(d) Money Laundering and Proceeds of Crime Act, 2013	S14(1) of the Money Laundering and Proceeds of Crime Act, 2013

been prescribed, meaning, by deduction, that full CDD measures must be undertaken for all occasional transactions and domestic or international wire transfer regardless of the amount involved. The failure to prescribe these thresholds places an unnecessary burden on reporting entities.

⁷⁶² See the footnote above.

⁷⁶³ Act 4 of 2013.

Section 10(1)(a) of Botswana's Financial Intelligence Agency Act 2009⁷⁶⁴ prohibits a specified party from establishing a business relationship or concluding a transaction with a customer unless the specified party has undertaken due diligence measures and such other steps as may be prescribed to establish and verify the identity of the customer. No threshold is prescribed in the Act and no reference is made to "occasional transactions."

Similarly, section 21(1) of the South African Financial Intelligence Centre Act 2001⁷⁶⁵ (As Amended) prohibits accountable institutions from establishing a business relationship or concluding a single transaction with a client unless the accountable institution has taken the prescribed steps to: establish and verify the identity of the client; if the client is acting on behalf of another person, to establish and verify the identity of that other person and the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and if another person is acting on behalf of the client, to establish and verify (i) the identity of that other person; and (ii) that other person's authority to act on behalf of the client.⁷⁶⁶

The wording of section 21 of the Financial Intelligence Centre Act 2001 (As Amended) is generally not compliant with FATF Recommendation 10 as it does not specifically address the carrying out of an occasional transaction above an applicable designated threshold (USD/EUR 15,000), including situations where the transaction is carried out in a single operation or several operations that appear to be linked. South Africa's approach to providing for these types of exemptions and the application of simplified CDD measures has not been to amend the Financial Intelligence Centre Act 2001 or the Money Laundering and Terrorist Financing Control Regulations (MLTFCR) but instead to issue a number of separately gazetted exemptions to sections of the Financial Intelligence Centre Act. These exemptions either require simplified CDD measures⁷⁶⁷ or exempt specified institutions, when issuing products that meet strict criteria from obtaining and verifying a customer's identification.⁷⁶⁸

While Namibia's Financial Intelligence Act 2012⁷⁶⁹ does not set a threshold for occasional transactions, paragraph 5 of Guidance Note No 2 of 2009 on Customer Identification and Record Keeping states that, "Accountable institutions should deploy customer due diligence measures **at all relevant times, particularly when:** establishing business relationships; carrying out single transactions above five thousand Namibian dollars (N\$5000.00), for casinos and other gaming institutions single transactions above twenty five thousand Namibian dollars (N\$25000.00)); there is a suspicion of money laundering; or the accountable institution has doubts about the veracity or adequacy of customer identification information or documentation provided by prospective clients or clients with whom a business relationship was established before the Act was commenced." The use of the words "Accountable institutions should deploy customer due diligence measures

⁷⁶⁴ Act 6 of 2009.

⁷⁶⁵ Act 38 of 2001 (As Amended).

⁷⁶⁶ Section 21(2) of Act 38 of 2001 (As Amended) reads, "Section 21(2) requires accountable institutions that had an already established business relationship with a client before the Act took effect not to conclude a transaction in the course of the business relationship, unless the accountable institution has taken the prescribed steps to: establish and verify the identity of the client; if another person acted on behalf of the client in establishing the business relationship, to establish and verify the identity of that other person and that other person's authority to act on behalf of the client; if the client acted on behalf of another person in establishing the business relationship, to establish and verify the identity of that other person and the client's authority to act on behalf of that other person; and to trace all accounts at that accountable institution that are involved in transactions concluded in the course of that business relationship."

⁷⁶⁷ See Exemption 17.

⁷⁶⁸ See the Prepaid Low Value Payment Product Exemption issued in 2010.

⁷⁶⁹ Act 13 of 2012.

at all relevant times, particularly when” seems to negate the possible reading of a proven low risk exemption into paragraph 5.

If however read with Section 2.1 of the General Exemption Order: Financial Intelligence Act, 2007, issued 5 May 2009 and paragraph 8(4) of Determination FICD 3, it is clear that such an exemption was intended by the drafters of the Guidance Note. Paragraph 8(4) of Determination FICD 3 reads, “reference is thus hereby made to Section 2.1 of the General Exemption Order: Financial Intelligence Act, 2007, issued 5 May 2009 which provides: ‘For purposes of regulation 2(3) of the Regulations, an accountable institution is exempt from establishing the identity of a client concluding a single cash transaction, subject to the condition that such single cash transaction is less than or equal to the amount determined by the Financial Intelligence Centre under section 13(1) of the Act.’ It is hereby determined that such amount is five thousand Namibian dollars for any accountable institution under Schedule 1 of the Act, except an accountable institution under item 8, namely, a person who carries on the business of a casino or gambling institution, and twenty-five thousand Namibian dollars for any accountable institution under item 8 of Schedule 1 of the Act, namely, any person who carries on the business of a casino or gambling institution.’

In terms of section 15(1) of Tanzania’s Anti-Money Laundering Act 2006⁷⁷⁰, a reporting person is required to take reasonable measures to satisfy himself as to the true identity of any applicant seeking to enter into a business relationship with him or to carry out a transaction or series of transactions with him, by requiring the applicant to produce an official record reasonably capable of establishing the true identity of the applicant.⁷⁷¹ The AMLA does not refer to an occasional transaction over an applicable designated threshold (USD 15,000) including situations where the transaction is carried out in a single operation or several operations that appear to be linked. Regulation 24 of the Tanzanian Anti-Money Laundering Regulations 2012 refers simply to “carrying out an occasional transaction.”

In Zambia, section 16(1)(b) of the Financial Intelligence Centre Act, 2010⁷⁷² requires reporting entities to identify and verify their customers' identities by means of reliable and independent source document or information when the customer, who is neither an account holder nor in an established business relationship with a financial institution, wishes to carry out a transaction in an amount equal to, or above, such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked: provided that if the amount of the transaction is unknown, the customer's identification shall be verified as soon as the amount of the transaction has reached the prescribed amount.” As far as we have been able to ascertain, the threshold mentioned in sections 16(1)(b) has not been prescribed, meaning, by deduction, that full CDD measures must be undertaken for all occasional transactions regardless of the amount involved. The failure to prescribe this threshold places an unnecessary burden on reporting entities.

The law and or regulations in force in Angola, the DRC, Lesotho, Malawi, Mauritius, Mozambique, Namibia, the Seychelles, South Africa, Swaziland and Zimbabwe contain a provision setting a threshold for an occasional transaction. This threshold amounts to a “Proven Low Risk Exemption” below which CDD measures are not required. As depicted in Table 61 below, most countries set this threshold well below the recommended FATF threshold of USD15, 000. The only country that has set the threshold for an occasional transaction at USD15, 000 is Angola.

⁷⁷⁰ Act 12 of 2006 (As Amended) . This Act is applicable to Mainland Tanzania only.

⁷⁷¹ Section 15(1)(a) Act 12 of 2006 (As Amended).

⁷⁷² Act 46 of 2010.

Table 61: Thresholds Applied (Occasional Transactions)

Country	Statutory Reference	Occasional Transaction Threshold (As Referenced in Law or regulation)	Occasional Transaction Threshold (USD Equivalent)
Angola	✓ Article 5(1)(b) Law n° 34/11	USD 15,000	USD 15,000
Botswana	✗ NA	No Threshold below which CDD is not required.	No Threshold
DRC	✓ Article 9 of Law n° 04/016	USD 10,000	USD 10,000
Lesotho	✓ S16(g)(d) Money Laundering and Proceeds of Crime Act, 2008 ⁷⁷³	M100, 000	USD 9654.15
Malawi	✓ Regulation 3(1)(b) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	K500,000	USD 1162.77
Mauritius	✓ Regulation 4(2)(c) Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	350,000 Rupees	USD 11606.92
Mozambique	✓ Article 10(1)(b)(i) and (ii) Law n° 14/2013	450,000 Meticalis	USD 14197.97
Namibia	✓ S2.1 General Exemption Order: Financial Intelligence Act, 2007, issued 5 May 2009 Paragraph 8(4) of Determination FICD 3	5000 Namibian Dollars	USD 478.51
Seychelles	✓ Regulation 5 and 8(1)(b) of the Anti-Money Laundering	SCR100,000 or SCR50,000 ⁷⁷⁴	USD 8277.68 and USD 4138.84

⁷⁷³ Act 4 of 2008.

⁷⁷⁴ Regulation 8(1)(b) of the Anti-Money Laundering Regulations 2012 requires reporting entities to undertake CDD measures when carrying out a one-off transaction. Regulation 5 defines a once off transaction as, “a transaction carried out other than as part of a business relationship that exceeds SCR100,000 or SCR50,000 in the case of cash transactions, whether the transaction is carried out in a single operation or several operations which appear to be linked.”

	Regulations 2012		
RSA	✓ Various Exemptions	Varies	Varies
Swaziland	✓ S7 Money Laundering and Financing of Terrorism (Prevention) Act 2011	E2,500	USD 239.01
Tanzania	✗ NA	No Threshold below which CDD is not required.	No Threshold below which CDD is not required.
Zambia	✗ NA	No Threshold below which CDD is not required.	No Threshold below which CDD is not required.
Zimbabwe	✓ S15(1)(b) Money Laundering and Proceeds of Crime Act, 2013 ⁷⁷⁵	USD 5000	USD 5000

Perhaps the most serious deficiency identified in several countries is the fact that the AML/CFT Law or Regulations do not contain a provision requiring financial institutions to undertake CDD measures when carrying out wire transfers. While several of these countries meet the requirements of FATF Recommendation 16 (Wire Transfers), the CDD provisions in several Acts make no mention of CDD being specifically required for wire transfers that are above the threshold of USD1, 000. Even fewer include the permitted de minimis threshold for occasional wire transfers, below which only the names of the originator and beneficiary and an account number / unique identifier are required.

The peculiar manner in which Article 10(1) of Mozambique’s new AML Law, Law n° 14/2013 is drafted provides an example of what can go wrong when FATF’s Recommendations and Interpretive Notes are incorrectly interpreted. Article 10(1) of Law n° 14/2013 requires financial institutions and non-financial bodies to identify their customers and confirm their identity through the presentation of valid documents every time they:

- Establish a business relationship;⁷⁷⁶
- Effect occasional transactions of amounts equal to or above four hundred and fifty thousand meticaís (i) when the total amount of the transaction is not known at the time of commencement of the operation, the financial entity must proceed with the identification as soon as the amount is known and verify if the threshold has been reached and (ii) in case of a domestic or international transfer;⁷⁷⁷
- If it is suspected that the transactions, independently of their value, are related to the crime of money laundering or funding of terrorist activities;⁷⁷⁸
- There are doubts as to the veracity or adequacy of the customer’s identification details.⁷⁷⁹

⁷⁷⁵ Act 4 of 2013.

⁷⁷⁶ Article 10(1)(a) Law n° 14/2013.

⁷⁷⁷ Article 10(1)(b)(i) and (ii).

⁷⁷⁸ Article 10(1)(c).

⁷⁷⁹ Article 10(1)(d).

The manner in which Article 10(1)(b) of Law n° 14/2013 is drafted appears to provide for a proven low risk exemption for both occasional transactions and domestic or international transfers below the threshold of 450, 000 Meticais (USD 14197.97).⁷⁸⁰ While the threshold of USD/EUR 15,000 for occasional transactions is suggested in FATF Recommendation 10, Recommendation 10 only allows for a proven low risk exemption for wire transfers in the circumstances covered by Recommendation 16 and its interpretive note. Interpretative Note 16, paragraph 5 states, "countries may adopt a de minimis threshold for cross-border wire transfers (no higher than USD/EUR 1,000) below which the following should apply:

- (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
- (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information."

As an amount is not specifically stated in Article 10(1)(b)(ii) of Law n° 14/2013 and the normal reading of the provision reads, "financial institutions and non-financial bodies must identify their customers and confirm their identity through the presentation of a valid document, every time they effect occasional transactions of amounts equal or superior to four hundred and fifty thousand meticaïs in case of a domestic or international transfer", it appears that the threshold of four hundred and fifty thousand meticaïs for domestic and international transfers is in direct contravention with the maximum de minimis threshold of USD 1,000 as set out in FATF Recommendations 10 and 16 and Interpretive Note 16.

Several countries AML/CFT Laws and or Regulations do not require financial institutions to undertake CDD measures when there is a suspicion of ML/TF of where the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Only the DRC's Law is deficient with respect to prohibiting anonymous accounts or accounts held in fictitious names.

9.1.2 Component B: Identification Measures and Verification Sources

The analysis in the tables below is focused on the first requirement of Component B of FATF Recommendation 10, namely, financial institutions are required to identify the customer and verify the customer's identity using reliable, independent source documents, data and information.⁷⁸¹ The sections and tables below set the required information from customers, acceptable documents and listed verification sources as they are found in each SADC Member States primary AML/CFT Law and or Regulations.

Table 62 below has been prepared by reviewing the AML/CFT Law, Regulations, Directives, Guidelines and Guidance Notes in each country and searching for required information as listed. As can be seen, all fourteen

⁷⁸⁰ Conmill.com. Accessed 04/06/2014.

⁷⁸¹ This report does not focus on the other components of Component B of Recommendation 10, namely identification of the beneficial owner, understanding the intended purpose of the business relationship and ongoing due diligence. Readers should refer to the individual country reports for information in this regard.

countries require the standard information such as full name, date of birth, identity number and nationality. Most require a residential address that must be verified through a variety of acceptable methods/independent verification sources. In some cases, a person’s nationality and identity number are not expressly included in the individual countries list of requirements but for the purposes of this analysis, the assumption has been made that if an ID book / card is required, then the full name, date of birth, identity number and nationality are required. Several countries actually state that official documents must contain a photograph, whilst others simply list documents (ID, passport) that always contain a photograph. For this reason, the assumption that photo ID is required by all has also been made. Tanzania is the only SADC country that requires both a signature and a finger print.⁷⁸² Only three countries, Angola, South Africa and Tanzania require a tax number should such be available. Although Regulation 3(1)(d) of the South African Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended) requires an accountable institution to obtain from, or in respect of, a natural person who is a citizen of, or resident in, the Republic, that person's income tax registration number, if such a number has been issued to that person, Exemption 6(2) exempts all accountable institutions from doing so.⁷⁸³ Four countries, Malawi, Namibia, Seychelles and Tanzania require additional contact information (postal address or email or phone number). It is interesting to note that the nature of income and or source of funds are only required by five countries and profession or occupation by six. The information requested, in particular occupation or source of income, nature and location of business activities, if any; and the source of funds involved in the transaction are recognised in most jurisdictions to seen to be a barrier to access to financial services. This is particularly so with respect to individuals that are not banked, trade informally and may not be in formal employment.

Table 62: Required CDD Information

Country	Statutory Reference	Full Name	Identity Number	Date of Birth	Photo on Doc.	Nationality	Residential Address	Postal Address, email, phone no.	Profession or Occupation	Nature Income or Source of Wealth	Tax Number	Signature
Angola See Annexure A, section A2.7.3.2	Article 5(3) of Law nº 34/11 Aviso nº 01/2011de	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗
Botswana See Annexure B, section B2.7.3.2	Section 10(3) Financial Intelligence Agency Act, 2009 ⁷⁸⁴	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗

⁷⁸²It is interesting to note that the Tanzanian Regulation is the only Regulation in the SADC region that requires reporting entities to acquire a signature and thumb print and to provide comprehensive instructions on how the thumb print is to be obtained.

⁷⁸³ See De Koker L and Symington J 2011 *Conservative Compliance Behaviour Drivers of Conservative Compliance Responses in the South African Financial Services Industry 17* where the authors state that, “the regulations also require institutions to obtain the income tax number (if issued) of a customer, but, simultaneously with the release of this requirement, an exemption [Exemption 6(2)] was issued that exempted institutions from obtaining the tax number.”

⁷⁸⁴ Act 6 of 2009.

DRC See Annexure C, section C2.7.3.2	Article 8 of Law n° 04/016	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Lesotho See Annexure D, section D2.7.3.2	Section 16(1) Money Laundering and Proceeds of Crime Act, 2008 ⁷⁸⁵ Paragraphs 6(2) and 6(3) Financial Institutions (Anti-Money Laundering) Guidelines, 2000	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
Malawi See Annexure E, section E2.7.3.2	Regulation 4(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Mauritius See Annexure F, section F2.7.3.2	Regulations 4 and 5 Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Mozambique See Annexure G, section G2.7.3.2	Article 10(4) Law n° 14/2013	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Namibia See Annexure H, section H2.7.3.2	Regulation 4 Financial Intelligence Regulations, 2009	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Seychelles See Annexure I, section I2.7.3.2	Guidelines on Anti-Money Laundering and Combatting the Financing of Terrorism Procedures for Reporting Entities, 2007	●	●	●	●	●	●	●	●	●	●	✗	✗

⁷⁸⁵ Act 4 of 2008.

RSA See Annexure J, section J2.7.3.2	Regulation 3(1) and 5(1) Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended) Exemption 6(2)	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗
Swaziland See Annexure K, section K2.7.3.2	6(2) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
Tanzania See Annexure L, section L2.7.3.2	Regulation 3 Anti-Money Laundering Regulations, 2012	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Zambia See Annexure M, section M2.7.3.2	Section 16(5)(a) Financial Intelligence Centre Act, 2010 ⁷⁸⁶	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Zimbabwe See Annexure N, section N2.7.3.2	Section 17 Money Laundering and Proceeds of Crime Act, 2013 ⁷⁸⁷	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗

Table 63 below sets out the types of Identification documents that are actually specified by each country. All fourteen countries list an ID Document or ID Card and most a Passport as the primary acceptable identification document. Other forms of identification documents such as driver’s licenses, birth certificates and voter’s cards are accepted in several jurisdictions. In some jurisdictions, passports are only acceptable forms of identification for non-citizens / foreigners while in others, passports are equally acceptable for both nationals/citizens and foreigners / non-citizens. From a financial inclusion perspective, the acceptance of alternative documents for identification and verification purposes is seen as a vital stepping stone to achieving a financially inclusive policy objective. It is therefore vital to note that law and regulation in only six SADC Member States, namely Malawi, Mozambique, Namibia, Seychelles, South Africa and Tanzania permit alternative documents.

Table 64 below lists the independent verification sources listed by each country in law, regulations and or guidelines. As can be seen, several countries have adopted alternative methods to verify information obtained such as an individual’s given residential address. The DRC, Mozambique, Namibia and Lesotho are notable

⁷⁸⁶ Act 46 of 2010

⁷⁸⁷ Act 4 of 2013.

exceptions as the legal and regulatory framework in these countries does not specifically list acceptable independent verification sources.

Table 63: Documents Listed

Country	Statutory Reference	ID Book/Card	Passport	Driving License	Voters Card	Birth Certificate	Alternative Docs Permitted
Angola See Annexure A, section A2.7.3.2	Article 5(3) of Law n° 34/11 Aviso n° 01/2011de	✓	✓	✗	✗	✗	✗
Botswana See Annexure B, section B2.7.3.2	S10(3) Financial Intelligence Agency Act, 2009 ⁷⁸⁸ Regulation 6 Banking (Anti-Money Laundering) Regulations, 1995	✓	✓	✗	✗	✗	✗
DRC See Annexure C, section C2.7.3.2	Article 8 of Law n° 04/016	✓	✓	✗	✗	✗	✗
Lesotho See Annexure D, section D2.7.3.2	S6(1)(b)(ii) Money Laundering and Proceeds of Crime Act, 2008 ⁷⁸⁹	✓	✓	✗	✗	✗	✗

⁷⁸⁸ Act 6 of 2009.⁷⁸⁹ Act 4 of 2008.

Malawi See Annexure E, section E2.7.3.2	Regulation 4(1)(b) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	✓	✓	✗	✗	✓
Mauritius See Annexure F, section F2.7.3.2	Regulation 4 of the Mauritian Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended) Paragraph 6.4.3 Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005	✓	✓	✓	✗	✗	✗
Mozambique See Annexure G, section G2.7.3.2	Article 10(4) Law n° 14/2013 Article 10(5) Law n° 14/2013	✓	✗	✗	✗	✗	✓
Namibia See Annexure H, section H2.7.3.2	Regulation 10 Financial Intelligence Regulations, 2009	✓	✓	✓	✗	✓	✓
Seychelles See Annexure I, section I2.7.3.2	Paragraph 8(ii) Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007	●	●	✗	✗	✗	●
RSA See Annexure J, section J2.7.3.2	Regulations 4 and 6 Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended)	✓	✓	✓	✗	✗	✓
Swaziland See Annexure K, section K2.7.3.2	Section 6(2) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓	✓	✗	✗	✗	✓

<p>Tanzania See Annexure L, section L2.7.3.2</p>	<p>Section 15(2) of Tanzania’s Anti-Money Laundering Act, 2006 (As Amended) Regulation 3(1) Anti-Money Laundering Regulations, 2012</p>	✓	✓	✓	✓	✓	✓
<p>Zambia See Annexure M, section M2.7.3.2</p>	<p>Section 16(2) of Zambia’s Financial Intelligence Centre Act, 2010⁷⁹⁰ Directive 6(1)(a) and (b) of the Bank of Zambia Anti-Money Laundering Directives, 2004</p>	✓	✓	✓	✗	✗	✗
<p>Zimbabwe See Annexure N, section N2.7.3.2</p>	<p>Section 24 of the Bank Use Promotion and Suppression of Money Laundering Act, 2004 (As Amended)⁷⁹¹ Paragraph 11.9.2 Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions and Non-Financial Businesses and Professions 2006</p>	✓	✓	✓	✗	✗	✗

⁷⁹⁰ Act 46 of 2010.

⁷⁹¹ [Chapter 24:24].

Table 64: Independent Verification Sources Listed

Country	Statutory Reference	None Listed	National Database or Register	Revenue Service	Credit Reference Agency	Rates or Utility Bill	Address validation & verification service	Personal visit to the home of the applicant	Reference from well-known professional/ government official	Reference or Affidavit from Employer	Bank Statement	Reference from a Bank	Reference from known customer of bank	Reference from Customary Authority	Telephone Book	Cellular or telephone account	Valid television license	Valid insurance policy	Lease or Tenancy Agreement
Angola See Annexure A, section A2.7-3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Botswana See Annexure B, section B2.7-3.2	Regulation 6 Banking (Anti-Money Laundering) Regulations, 1995	NA	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗
DRC See Annexure C, section C2.7-3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Lesotho See Annexure D, section D2.7.3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	
Malawi See Annexure E, section E2.7.3.2	Regulation 10 Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	NA	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
Mauritius See Annexure F, section F2.7.3.2	Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005	NA	✗	✗	✗	●	✗	✗	✗	✗	●	●	✗	✗	✗	✗	✗	✗	✗	✗
Mozambique See Annexure G, section G2.7.3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Namibia See Annexure H, section H2.7.3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Seychelles See Annexure I, section I2.7.3.2	Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007 ⁷⁹²	NA	●	✗	●	●	✗	✗	✗	✗	●	✗	✗	✗	●	✗	✗	✗	✗
RSA See Annexure J, section J2.7.3.2	Regulations 4 and 6 Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended) Paragraphs 7 and 11 of Guidance Note 3 Guidance for Banks on Customer Identification and Verification and Related Matters (2005)	NA	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓
Swaziland See Annexure K, section K2.7.3.2	NA	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

⁷⁹² The Seychelles Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007 which were issued by the Financial Intelligence Unit in December, 2007 require that the residential address be verified and suggests that the best way of verifying the address is: to request a recent (not older than 3 months) copy of utility bills for an individual and exert from the Chamber of Commerce for a legal entity; by checking an official register such as the voters roll and Social Security Register; by making a credit reference agency search; by requesting sight of a recent utility bill, local authority tax bill, bank or other financial institution bank statement; or by checking a local and current telephone directory.

<p>Tanzania</p> <p>See Annexure L, section L2.7.3.2</p>	<p>Regulation 3 Anti-Money Laundering Regulations, 2012</p>	<p>NA</p>	<p>✘</p>	<p>✓</p>	<p>✘</p>	<p>✓</p>	<p>✘</p>	<p>✘</p>	<p>✓</p>	<p>✓</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✓</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>
<p>Zambia</p> <p>See Annexure M, section M2.7.3.2</p>	<p>Directive 7B the Bank of Zambia Anti-Money Laundering Directives, 2004</p>	<p>NA</p>	<p>✘</p>	<p>✘</p>	<p>✓</p>	<p>✓</p>	<p>✓</p>	<p>✘</p>	<p>✓</p>	<p>✓</p>	<p>✘</p>	<p>✘</p>	<p>✓</p>	<p>✓</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>
<p>Zimbabwe</p> <p>See Annexure N, section N2.7.3.2</p>	<p>Paragraph 11.9.6 Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions and Non-Financial Businesses and Professions 2006</p>	<p>NA</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>●</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>●</p>	<p>●</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>	<p>✘</p>

The approaches taken by South Africa, Malawi and Zambia are highlighted below as approaches that should be considered by other SADC Member States.

In South Africa, the Money Laundering and Terrorist Financing Control Regulations⁷⁹³ require an Accountable Institution to verify the full names, date of birth and identity number of a natural person by comparing these particulars with an identification document of that person (Regulation 4(1)(a)(i)); or in the case where that person is, for a reason that is acceptable to the institution, unable to produce an identification document, another document issued to that person, which, taking into account any guidance notes concerning the verification of identities which may apply to that institution, is acceptable to the institution and bears: a photograph of that person (Regulation 4(1)(a)(ii)(aa)); that person's full names or initials and surname (Regulation 4(1)(a)(ii)(bb)); that person's date of birth (Regulation 4(1)(a)(ii)(cc)), and that person's identity number (Regulation 4(1)(a)(ii)(dd)). Accountable institutions are also required to verify the income tax registration number by comparing this number with a document issued by the South African Revenue Service bearing such a number and the name of the natural person (Regulation 4(2)).⁷⁹⁴ Paragraph 11 of Guidance Note 3: lists examples of acceptable documents that can be used to verify the residential address of a natural person. These should be less than three months old and include:

- a utility bill reflecting the name and address of the person;
- a bank statement from another bank reflecting the name and residential address of the person;
- a recent lease or rental agreement reflecting the name and residential address of the person;
- municipal rates and taxes invoice reflecting the name and residential address of the person;
- telephone or cellular account reflecting the name and address of the person; and
- a valid television license reflecting the name and residential address of the person;
- a recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the person.

It is important to note that paragraph 7 of Guidance Note 3 states further that: "If none of the above is available banks may explore other means to verify a client's address such as an affidavit containing the following particulars from a person co-habiting with the client or an employer of the client: name, residential address, identity number of the client and the deponent of the affidavit; relationship between the client and the deponent of the affidavit; and confirmation of the client's residential address."

The approach taken by Malawi with respect to identification measures and verification sources needs to be highlighted as an example of how countries can approach two problems particularly relevant in the African context. These are: 1) the lack of a National Identification System; and 2) the lack of formal addresses in many parts of the country.

In Malawi, Regulation 4(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to identify a natural person that is a Malawian citizen by obtaining the following particulars:

- (a) his full name;
- (b) his national identity card, passport or driving license indicating the person's date of birth;

⁷⁹³ Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended).

⁷⁹⁴ This requirement is however neutralised by Exemption 6(2).

- (c) his physical address including street names and plot number or a detailed description of the location named in Malawi where the physical address is not available;
- (d) his village, traditional authority and district of origin where applicable;
- (e) his postal address, email address and telephone contacts where applicable;
- (f) his occupation or source of income and expected level of monthly income;
- (g) nature and detailed description of the location of business activities or place of employment, whichever is applicable; and
- (h) purpose and intended nature of the business relationship.

Malawi does not have a National Identification system and as such, the production of accepted identification documentation in compliance with the CDD requirements set out in the AML Act has the potential to present problems for customers, banks and other NBFIs alike. However, the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 incorporates Malawi's financial inclusion agenda and allows for the acceptance of unofficial identification documents on a risk-based approach. Although Regulation 4 allows for alternative means of providing ones address, Regulation 4(1)(c) reads 'his physical address including street names and plot numbers, or a detailed description of the location named in Malawi where the physical address is not available', Malawian citizens are still required to produce an accepted form of identification which is listed in Regulation 4(1)(b) as 'his national identity card, passport or driving licence, indicating the person's date of birth'. The FIU however stated that letters of introduction from the District Commissioner and other Traditional Authorities are however accepted as forms of identification. The Regulation also makes use of the words 'where applicable' with respect to obtaining details of the persons 'village, traditional authority and district of origin', 'postal address, e-mail address and telephone contacts', implying that where such details are not applicable, they are not required.

Regulation 4(1)(g) is also particularly relevant in the African context. This requires Malawian citizens to provide the 'nature and detailed description of the location of business activities or place of employment, whichever is applicable.' This provision is wide enough to include informal traders who trade on the street corner and does not limit this context to those formally employed.

Regulation 10 which deals with the verification of details required in regulation 4(1) and 4(2) makes use of the words "where practical but not limited to" and reads 'A financial institution shall independently verify the particulars and details referred to in regulation 4(1) and (2) in respect of a natural person who is a citizen or a resident in Malawi, where practical but not limited to, by obtaining – (a) a letter from his employers, stating the current monthly salary; (b) current payslip; (c) utility bills; (d) city rates bills; (e) lease agreement; or (f) tenancy agreement', which on the normal interpretation of the wording implies that if it is not practical to make use of these sorts of documents, then other 'creative' means of verifying details may suffice.

In terms of the Bank of Zambia Anti-Money Laundering Directives, 2004, verification of names and addresses of individual customers must be undertaken through one or more of the following methods:

- by obtaining a reference from a professional, an employer of the individual customer, a known customer of the regulated institution, or a customary authority that knows the applicant all of whom should have known the applicant for not less than one year⁷⁹⁵;
- in the case of non-residents, obtaining references
- from the individual customer's foreign banks, where possible⁷⁹⁶;

⁷⁹⁵Directive 7B(a) Anti-Money Laundering Directives, 2004.

- by conducting a credit reference agency search⁷⁹⁷;
- by requesting an original or certified true copy of recent council or applicable rates or utility bill receipt⁷⁹⁸;
- by using one of the address validation or verification services on offer⁷⁹⁹; or
- in addition to one or more of the above, doing all things that the regulated institution may deem necessary to verify the documentation submitted by the applicant.⁸⁰⁰

CB Circular No: 04/2011 which is a Practice Note on Anti-Money Laundering Customer Due Diligence was published by the Bank of Zambia on the 7th October 2011 in response to the identified issue that some financial service providers in interpreting the Bank of Zambia Anti-Money Laundering Directive, 2004 on address verification, were restricting themselves to the listed requirements provided in Directive, 7B(a) - (e). Circular No: 04/2011 makes it quite clear that Directive 7B(f) provides flexibility in the options a regulated financial service provider can employ to verify both Identity and address of a customer, and as such, the options should not necessarily be taken to be limited to options listed in Directive 7B(a) - (e). In line with the flexibility provided by the FATF Recommendations, the Circular specifically states that:

“It may, for instance, be sufficient for the regulated institution to be furnished with confirmation from a civic leader, church leader, school head teacher, traditional ruler or other lawfully recognised leaders that the customer resides within the locality that such ruler or leader presides. The financial service providers must therefore, develop policies and operational procedures that will guide staff in their fulfillment of the due diligence requirements.”

9.1.3 Component C: The Timing and Verification of Identity

The law or regulation in six countries, namely Botswana, the DRC, Lesotho, Mozambique, Swaziland and Tanzania does not contain a provision or regulation permitting institutions to complete verification as soon as is reasonably practicable after the establishment of a relationship where ML/TF risks are managed and it is essential not to interrupt the normal course of business. While section 16(4) of the Zambian Financial Intelligence Centre Act, 2010⁸⁰¹ states that the Minister may prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of the business relationship if: (a) the risk of money laundering or financing or terrorism is effectively managed; and (b) a delay in the verification is essential not to interrupt the normal conduct of business, at the time of writing of this report, as far as we are aware, these ‘circumstances’ had not been prescribed by the Minister. Likewise, section 16(1) of Zimbabwe’s Money Laundering and Proceeds of Crime Act, 2013⁸⁰² states that the Director may, through a directive, prescribe the circumstances in which the verification of identity may be completed as soon as reasonably practicable after the commencement of business if the risk of money laundering or financing of terrorism is effectively managed and a delay in the verification process is unavoidable in the interests of not interrupting the normal conduct of business.⁸⁰³ At the time of the writing of this report, no such directive had been issued.

⁷⁹⁶ Directive 7B(b).

⁷⁹⁷ Directive 7B(c).

⁷⁹⁸ Directive 7B(d).

⁷⁹⁹ Directive 7B(e).

⁸⁰⁰ Regulation 7B(f).

⁸⁰¹ Act 46 of 2010.

⁸⁰² Act 4 of 2013.

⁸⁰³ Section 16(1)(a) and (b).

Four countries do not explicitly require financial institution that are unable to comply (subject to appropriate modification of the extent of measures on a risk-based approach) not to open an account, commence business relations or perform the transaction and consider submitting a Suspicious Transaction Reporting (STR).

Table 65: Timing and Verification of Identity

Country	Financial institutions are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers	The AML Law and or Regulations permit institutions to complete verification as soon as is reasonably practicable after the establishment of a relationship where ML/TF risks are managed and it is essential not to interrupt the normal course of business	Where financial institution is unable to comply (subject to appropriate modification of the extent of measures on a risk-based approach) it is required not to open an account, commence business relations or perform the transaction and should consider submitting a STR.
Angola See Annexure A, section A2.7.3.3	✓ Article 6(1) Law n° 34/11	✓ Article 6(2) Law n° 34/11	✓ Article 11 Law n° 34/11
Botswana See Annexure B, section B2.7.3.3	✓ S10 Financial Intelligence Agency Act, 2009 ⁸⁰⁴	✗	✗
DRC See Annexure C, section C2.7.3.3	✓ Article 8 of Law n° 04/016	✗	✗
Lesotho See Annexure D, section D2.7.3.3	✓ S16 Money Laundering and Proceeds of Crime Act, 2008 ⁸⁰⁵	✗	✗
Malawi See Annexure	✓ S24 (1) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁸⁰⁶	✓ ⁸⁰⁷ Regulation 9(2) Money Laundering, Proceeds of	✓ Section 25 (1) Money Laundering Proceeds of Serious Crime and Terrorist Financing

⁸⁰ Act 6 of 2009.

⁸⁰⁵ Act 4 of 2008.

E, section E2.7.3.3	Regulation 9(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	Serious Crime and Terrorist Financing Regulations, 2011	Act, 2006 ⁸⁰⁸ Regulation 3(9) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011
Mauritius See Annexure F, section F2.7.3.3	✓ Regulation 11 of the Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓ ⁸⁰⁹ Paragraph 4.6 Code on the Prevention of Money Laundering and Terrorist Financing, 2012	✓ Regulation 12 of the Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)
Mozambique See Annexure G, section G2.7.3.3	✓ Article 11 of Law n° 14	✗	✓ Article 10(2)(f) of Law n° 14/2013
Namibia See Annexure H, section H2.7.3.3	✓ S22 Financial Intelligence Act, 2012 ⁸¹⁰	✓ ⁸¹¹ Regulation 3(3) of the Financial Intelligence Regulations, 2009	✓ S22(2) Financial Intelligence, 2012 ⁸¹²
Seychelles See Annexure I, section I2.7.3.3	✓ Regulation 10(1) Anti-Money Laundering Regulations, 2012	✓ Regulation 10(2) of the Anti-Money Laundering Regulations, 2012	✓ S5 Anti-Money Laundering Act, 2006 (As Amended) ⁸¹³

⁸⁰⁶ Act 11 of 2006.

⁸⁰⁷ Regulation 9(2) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 permits financial institutions to adopt a deferred approach to customer verification. If a financial institution establishes a business relationship prior to verification, financial institutions are required, in line with a risk based approach, to limit the number, type and amount of transactions that can be performed. This deferred verification is however only permitted if the financial institution has effective risk management systems. In the absence of such, the financial institution is not permitted to enter into a business relationship before the customer's identity has been verified. This seems to be in direct contrast with section 100(1) of the Financial Services Act, 2010 which contains the words "a financial institution in Malawi shall demand proof of and record the identity of its clients or customers."

⁸⁰⁸ Act 11 of 2006.

⁸⁰⁹ It must be pointed out that the Code does not apply to banks as it was issued by the FSC and is applicable to financial service providers licensed under the Financial Services Act 2007, Insurance Act 2005 and Securities Act 2005 and is also applicable to the designated non-financial businesses and professions (DNFBPs) licensed by the FSC, namely Management Companies and Corporate Trustees..

⁸¹⁰ Act 13 of 2012.

⁸¹¹ Regulation 3(3) of the Financial Intelligence Regulations, 2009 states that, "despite anything to the contrary in these regulations, an accountable institution may establish a business relationship, or take any preparatory steps to conclude a single transaction, before verifying the identity of a client, but must comply with the provisions regarding verification of such client's identity in accordance with these regulations prior to such client receiving any benefit from such transaction" implying that CDD measures may be deferred.

⁸¹² Act 13 of 2012.

⁸¹³ Act 5 of 2006.

RSA See Annexure J, section J2.7.3.3	✓ Section 21 Financial Intelligence Centre Act, 2001 (As Amended) ⁸¹⁴	✓ Included in various Exemptions and PCCs.	✗ ⁸¹⁵
Swaziland See Annexure K, section K2.7.3.3	✓ S6(1) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✗	✓ Section 7 Money Laundering and Financing of Terrorism (Prevention) Act 2011
Tanzania See Annexure L, section L2.7.3.3	✓ Section Act 15(1) Anti-Money Laundering Act, 2006 (As Amended) ⁸¹⁶	✗	✓ Regulation 17(c) of the Anti-Money Laundering Regulations, 2012
Zambia See Annexure M, section M2.7.3.3	✓ S16(3) Financial Intelligence Centre Act, 2010 ⁸¹⁷	* S16(4) Financial Intelligence Centre Act, 2010	✓ S21 Financial Intelligence Centre Act, 2010
Zimbabwe See Annexure N, section N2.7.3.3	✓ S16(1) Money Laundering and Proceeds of Crime Act, 2013 ⁸¹⁸	* S16(1) Money Laundering and Proceeds of Crime Act, 2013	✓ S22 Money Laundering and Proceeds of Crime Act, 2013

9.1.4 The Risk-Based Approach to CDD: The Proven Low Risk Exemption and Simplified Measures

The AML Law and or Regulations in ten countries mandates the adoption of [a risk-based approach](#), either directly or through inference. Most jurisdictions in SADC started with a purely rules based approach to AML and have slowly introduced the concept of the risk-based approach (RBA) through regulations, exemptions,

⁸¹⁴ Act 38 of 2001 (As Amended).

⁸¹⁵ Neither the Financial Intelligence Centre Act, 2001 (As Amended) nor the MLTFCR make any reference to the FATF requirement that where a financial institution is unable to comply with the applicable CDD requirements that it should be required to terminate the business relationship and consider making a suspicious transaction report in relation to the customer.

⁸¹⁶ Act 12 of 2006 (As Amended).

⁸¹⁷ Act 46 of 2010.

⁸¹⁸ Act 4 of 2013.

guidelines and guidance notes. Two countries, namely Namibia and South Africa have elected not to amend their primary AML Acts through the insertion of sections covering the adoption of a RBA, but have instead issued separately gazetted exemptions to sections of the AML Act. Four countries, namely Botswana, DRC, Lesotho and Swaziland make no mention of the requirement to adopt a RBA in legislation or regulation or guidelines.

Table 66: Risk Based Approach Mandated in Law or Regulation

Country	Statutory Reference	Law/Regs specifically mandate adoption RBA	Comment
Angola See Annexure A, section A2.7.3.4	Article 8(1) Law n° 34/11	✓	Reporting entities in Angola are permitted to adapt the nature and extent of the verification procedures and due diligence measures based on the risk associated with the client, the business relationship, the transaction and the origin or destination of the funds. Reporting entities must however be in a position to prove the adaptation of the procedures adopted, whenever they are requested to do so by competent supervisory authorities.
Botswana See Annexure B, section B2.7.3.4	None	✗	The Financial Intelligence Agency Act, 2009 ⁸¹⁹ does not contain any provisions specifically mandating the adoption of the RBA.
DRC See Annexure C, section C2.7.3.4	None	✗	Law n° 04/016 does not mandate the adoption of a risk based approach nor does it contain any provisions related to simplified measures that may be undertaken by credit institutions and other specified parties in proven lower risk situations. Law n° 04/016 does however include an exemption for occasional transactions.
Lesotho See Annexure D, section D2.7.3.4	None	●	A meeting with the Bankers Association of Lesotho confirmed that the CDD measures are the same for all customers and that a tiered or progressive approach has not been introduced. The Financial Institutions (Know Your Customer) (KYC) Guidelines 2007 do however classify business relationships with customers on the basis of risk as provided for under Part IV (Customer Categorisation). Paragraph 15(3) requires financial institutions to have in place a system of periodical review of risk levels of accounts and apply enhanced due diligence measures depending on the level of risk. It does not however require financial institutions to specifically apply enhanced due diligence on high risk customers or simplified measures to low

⁸¹⁹ Act 6 of 2009.

			risk customers.
Malawi See Annexure E, section E2.7.3.4	Regulation 3(5) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁸²⁰ does not contain a specific provision mandating the adoption of a RBA. The Money Laundering Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 s references the adoption of the RBA.
Mauritius See Annexure F, section F2.7.3.4	Paragraph 5.4 of the Code on the Prevention of Money Laundering and Terrorist Financing, 2012	✓	The Financial Intelligence and Anti-Money Laundering Act, 2002 ⁸²¹ does not specifically mandate the adoption of a RBA. Paragraph 5.4 of the Code on the Prevention of Money Laundering and Terrorist Financing, 2012 deals with low risk relationships and states “where the risk of money laundering or the financing of terrorism is lower and where information on the identity of the applicant for business is publicly available or where adequate checks and controls exist elsewhere in the national systems, it might be reasonable for Licensees to apply simplified or reduced due diligence measures when identifying and verifying the identity of the applicant for business.” ⁸²²
Mozambique See Annexure G, section G2.7.3.4	Article 10(2)(d) of Law n ^o 14/2013	✓ (Implied)	While Article 10(2)(d) of Law n ^o 14/2013 requires financial institutions and non-financial bodies to, “establish risk management systems to determine if the customer or the actual beneficiaries of a transaction are politically exposed individuals”, the law does not contain any specific articles detailing simplified measures for lower risk customers and products.
Namibia See Annexure H, section H2.7.3.4	Section 23 (1) of the Financial Intelligence Act 2012 ⁸²³ Guidance Note No. 4 of 2009	✓	The Financial Intelligence Act 2012 does not contain a specific provision on the requirement to adopt a RBA, however, this may be inferred by section 23 (1) of the Financial Intelligence Act 2012 that requires accountable institutions to have appropriate risk management and monitoring systems in place to identify clients or beneficial owners whose activities may pose a risk of money laundering, financing of terrorism, or both. In addition, in terms of the Exemption Order No. 75: General Exemptions: Financial Intelligence Act, 2007, under specific circumstances, an accountable institution is exempt from the establishing identity of a client, from keeping records, from reporting to FIC and from implementing compliance programmes.
Seychelles	Regulation 8(3) Anti-	✓	Regulation 8(3) of the Anti-Money Laundering Regulations, 2012 provides additional

⁸²⁰ Act 11 of 2006.

⁸²¹ Act 6 of 2002.

⁸²² The simplified CDD measures set out in paragraph 5.4 cover only regulated bodies (NBFIs) and not individual customers. No provision is made for lower CDD measures for potentially low risk products, services, transactions of delivery channels and no mention is made of financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access for financial inclusion purposes.

⁸²³ Act 13 of 2012.

See Annexure I, section I2.7.3.4	Money Laundering Regulations, 2012		requirements with respect to the CDD measures that must be applied on a risk-sensitive basis and states that a reporting entity shall determine the extent of customer due diligence measures on a risk-sensitive basis depending on (i) the type of customer, business relationship, product or transaction; and (ii) the guidelines issued by the FIU which are not inconsistent with the Act or the Regulations. Reporting entities must be able to demonstrate to their supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering, financing of terrorism or other criminal conduct.
RSA See Annexure J, section J2.7.3.4	Various	✓	The Financial Intelligence Centre Act, 2001 (As Amended) (FICA) is purely a rules based Act and makes not reference to the adoption of a RBA. However, South Africa has issued a number of separately gazetted exemptions to sections of the FICA. A number of Guidance Notes requiring accountable institutions to adopt a RBA have also been published.
Swaziland See Annexure K, section K2.7.3.4	None	✗	The Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not specifically mandate the adoption of a RBA.
Tanzania See Annexure L, section L2.7.3.4	Regulations 28(8) and 28(g) of the Anti- Money Laundering Regulations, 2012	✓	Regulations 28(8) and 28(g) of the Anti-Money Laundering Regulations, 2012 require a reporting person to “determine the extent of customer due diligence measures on a risk sensitivity basis depending on the type of customer, business relationship, product or transaction; and be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.”
Zambia See Annexure M, section M2.7.3.4	Section 16(7) of the Financial Intelligence Centre Act, 2010 ⁸²⁴	✓	Section 16(7) of the Financial Intelligence Centre Act, 2010 introduces the concept of a risk-based approach to CDD and reads: “A reporting entity shall apply the identification and verification requirements stipulated under subsections (1) and (5) to customers and beneficial owners with which it had a business relationship at the time of coming into force of this Act on a risk sensitive basis depending on the type and nature of the customer, business relationship, product or transactions, or as may otherwise be prescribed by the Minister.” This particular provision refers to “customers and beneficial owners with which it had a business relationship at the time of coming into force of this Act” and no mention of a risk-based approach when acquiring new customers, new products or transactions is made. The intention that reporting entities should adopt a risk-based approach to new business can

⁸²⁴ Act 46 of 2010.

			<p>however be inferred by section 18 (customers not physically present), section 19 (high-risk customers), and section 20 (identification and account opening for cross-border correspondent banking relationships). All of these sections refer to situations where enhanced due diligence measures should be taken. The Financial Intelligence Centre Act, 2010 is silent on simplified measures for low risk customers and products and no exemptions to the Act have been passed. Although CB Circular No: 04/2011 makes it clear that reporting entities are permitted to verify the identity of potential customers through “alternative forms of verification”, this is the only official statement that has been made by the Bank of Zambia on lighter CDD measures.⁸²⁵</p>
<p>Zimbabwe</p> <p>See Annexure N, section N2.7.3.4</p>	<p>Money Laundering and Proceeds of Crime Act, 2013⁸²⁶ Paragraphs 2.3.7 and 2.3.8 of the Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012</p>	<p>✓</p>	<p>Section 20 of the Money Laundering and Proceeds of Crime Act, 2013 requires enhanced CDD for high-risk customers and politically exposed persons. The Money Laundering and Proceeds of Crime Act, 2013 A does not contain any specific sections detailing simplified measures for lower risk customers and products. However, several sections of the Money Laundering and Proceeds of Crime Act, 2013 refer to the application of provisions on a risk sensitive basis depending on the type and nature of the customer, business relationship or products and transactions. Importantly, paragraphs 2.3.7 and 2.3.8 of the Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Money Transfer Agencies and Bureaux de Change, 2012 which were issued under the Bank Use Promotion and Suppression of Money Laundering Act (As Amended)⁸²⁷ state that:⁸²⁸</p> <p>“A designated institution is allowed to apply reduced or simplified identification measures where the risk of money laundering or terrorist financing is lower. The measures should be documented and must be approved by the board. Where the simplified CDD measures are subject to certain conditions being met, it is necessary to verify that these conditions apply,</p>

⁸²⁵ See Bankable Frontier Associates 2012 *Mapping the Retail Payment Services Landscape: Zambia* 46 where it is noted that, the Bank of Zambia “has also exercised some flexibility by allowing simpler KYC for Zanaco’s Xapit account, counterbalanced by account limits. However, these ad hoc actions have not had great impact on market practices, which continue to be overly conservative, something that is quite common in other countries. Also, the market continues to point to AML regulations as one of the most important burdens for financial inclusion, without having stated what exactly the burden is. The Bank of Zambia could consider issuing specific regulations to clarify this further, by exempting low-risk accounts from some requirements such as verification. Ideally, the Bank of Zambia should consider creating a tiered AML/CFT framework, which would be applicable to banks and nonbanks. An explicit tiered approach would give the market more confidence to implement lower controls for low-value accounts, and address the argument that AML is an obstacle.”

⁸²⁶ Act 4 of 2013.

⁸²⁷ [Chapter 24:24].

⁸²⁸ It is interesting to note that the cover page of the Guidelines states that “the guidelines are issued in terms of the Act and are legally binding, laying down minimum standards on Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change” as guidelines issued in other jurisdictions are not legally binding and are used by supervisory authorities as a moral suasion tool.

			<p>and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. In addition, information beyond customer identity, such as customer location and purpose of the transaction, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a customer should be sufficient to determine whether to go further, and in many cases customer monitoring will provide additional information.”</p>
--	--	--	---

As depicted in Table 67 below, several SADC countries in fact include proven low risk exemptions either directly in their primary AML law or regulations or have issued specific exemptions from provisions of the primary AML Act. Others allow for simplified measures in lower risk scenarios.

Table 67: Exemptions or Simplified CDD in Law or Regulation

Country	Institution	Product / Transaction	Customer	Value	Statutory Reference	Category	Measure (Simplified CDD / Proven Low Risk Exemption)
Angola See Annexure A, section A2.7.3.4	✓	✗	✗	✗	Article 9 of Law n° 34/11	A State or a public corporation, of any kind, that is part of the central or local administration Client is a public authority or organ that is subject to transparent accounting practices and object of audit. ⁸²⁹	Simplified CDD
Angola See Annexure A, section A2.7.3.4	✗	✓	✗	✓	Article 5(1)(b) Law n° 34/11	Occasional transactions below USD15,000	Proven Low Risk Exemption
Botswana See Annexure B, section B2.7.3.4	✓	✗	✗	✗	16A(4)Proceeds of Serious Crime Act 1990(As Amended) ⁸³⁰	Designated body or a body corresponding to a designated body in a state or country prescribed from the time being by the Minister as not applicable.	Proven Low Risk Exemption

⁸²⁹ Simplified due diligence is specifically provided for in Article 9 of Law n° 34/11 which allows reporting entities to apply simplified measures when there is a clear and demonstrated lower risk of money-laundering or the financing of terrorism and there is no suspicion of either. The mandate to apply simplified due diligence measures is however limited to when the client is the State or a public corporation, of any kind, that is part of the central or local administration and where the client is a public authority or organ that is subject to transparent accounting practices and object of audit.

⁸³⁰ Act 19 of 1990.

Botswana See Annexure B, section B2.7.3.4	✓	✓	✗	✓	Section 16A(8) Proceeds of Serious Crime Act, 1990 (As Amended)	Long term insurance where – (a) he amount of the periodic premiums to be paid in respect of the life policy in any 12 month period does not exceed the amount prescribed in Regulations (b) single premium to be paid in respect of a life policy does not exceed the amount prescribed in Regulation ⁸³¹	Simplified CDD ⁸³²
DRC Annexure C, section C2.7.3.4	✗	✓	✗	✓	Article 9 of Act 04/016	The identification of one-time clients shall be effected in accordance with the terms set out in Article 8 paragraph 2, for any transaction involving an amount in Congolese francs equal to or in excess of, 10,000 US dollars.	Proven Low Risk Exemption for occasional transactions below USD10,000
Lesotho Annexure D, section D2.7.3.4	✗	✓	✗	✓	Section 16(g)(d) Money Laundering and Proceeds of Crime Act, 2008 ⁸³³	Section 16(g)(d) provides and exemption for occasional transactions below M100, 000 and reads, “nothing in this section shall require the production of any evidence of identity where the transaction is an occasional transaction not exceeding M100,000 or any amount as may be prescribed by the Minister by notice in a Gazette, unless the accountable institution has reason to suspect that the transaction is suspicious or unusual.”	Proven Low Risk Exemption for occasional transactions below M100,000
Malawi Annexure E, section E2.7.3.4	✓	✗ ⁸³⁴	✓	✗	Regulation 3(5) Money Laundering, Proceeds of Serious Crime and Terrorist	Regulation 3(5) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 permits a financial institution to apply simplified customer identification requirements for: (a) financial institutions subject to the Regulations; (b) public companies that are subject to regulatory disclosure requirements; (c)	Simplified CDD Lower Risk Scenario

⁸³¹ In terms of section 9, paragraph (a) of subsection 8 excludes (a) a person scheme taken out by virtue of a contract of employment or the occupation of the person to be insured under the life policy provided that the life policy in question does not contain a surrender and may not be used as collateral (b) a transaction or series of transactions taking place in the course of long term insurance business in respect of which payment is made from an account held in the name of the other party with a designated body or a body corresponding to a designated body prescribed under subsection (4).

⁸³² Exempted from s16A(6) and s16A(7) that require institutions to obtain the required proof of the identity of the person.

⁸³³ Act 4 of 2008.

⁸³⁴ The Regulation does not however to low risk products with specific requirements and limits, although upon a broad interpretation of the wording, this may be inferred.

					Financing Regulations, 2011	customers whose average monthly income does not exceed K50,000; (d) other forms of low risk categories of customers, beneficial owners, beneficiaries or business relationships. ⁸³⁵	
Malawi Annexure E, section E2.7.3.4	x	✓	x	✓	Regulation 3(1)(b) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	Regulation 3(1) requires a financial institution to establish the identity of every customer when - (b) in the absence of a continuing business relationship, conducts any transaction exceeding K500,000; (c) carrying out several transactions within fourteen days, which appear to be linked and when consolidated, add up to K500,000.	Proven Low Risk for occasional transactions below K500,000
Malawi Annexure E, section E2.7.3.4	✓	✓	✓	✓	Regulation 9(2) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	Regulation 9(2) permits financial institutions to adopt a deferred approach to customer verification. If a financial institution establishes a business relationship prior to verification, financial institutions are required, in line with a risk based approach, to limit the number, type and amount of transactions that can be performed. This deferred verification is however only permitted if the financial institution has effective risk management systems. In the absence of such, the financial institution is not permitted to enter into a business relationship before the customer's identity has been verified. ⁸³⁶	Deferred (Tiered) CDD
Mauritius Annexure F, section F2.7.3.4	x	✓	x	✓	Regulation 4(2)(c) Financial Intelligence and Anti-Money Laundering	CDD measures are required: in respect of a one-off transaction, where payment is to be made by, or to the applicant for business of an amount in excess of 350,000 rupees or an equivalent amount in foreign currency; and in respect of 2 or more once-off	Proven Low Risk Exemption

⁸³⁵ Regulation 3(6) reads "notwithstanding the provisions of sub-regulation (5) above, simplified or reduced customer identification requirements shall not be applied where there is a suspicion of money laundering or terrorist financing."

⁸³⁶ This seems to be in direct contrast with section 100(1) of the Financial Services Act, 2010 which contains the words "a financial institution in Malawi shall demand proof of and record the identity of its clients or customers."

					Regulations 2003 (As Amended)	transactions, where it appears at the outset or subsequently to a relevant person dealing with any of the transactions, that the transactions are linked and that the total amount, in respect of all of the transactions, which is payable by or to the applicant for business is in excess of 350,000 rupees or an equivalent amount in foreign currency.	
Mauritius Annexure F, section F2.7.3.4	●	●	✘	✘	Paragraph 6.98(a) and (b) Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005	Public companies listed on a recognised, designated and approved Stock/Investment Exchange Parastatal bodies in Mauritius Once-off transactions in which the proceeds of the transaction are not paid but are directly reinvested on behalf of the person to whom the proceeds are payable in another transaction. ⁸³⁷	Proven Low Risk Exemption
Mauritius Annexure F, section F2.7.3.4	●	●	✘	✘	Paragraph 6.99 Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005	Identification procedures are not required in relation to a one-off transaction, in which the proceeds of the transaction are not paid, but are directly reinvested on behalf of the person to whom the proceeds are payable in another transaction – (i) of which a record is kept; and (ii) which results only in another reinvestment made on that person's behalf or, in payment made directly to that person.	Proven Low Risk Exemption
Mauritius	✓	✘	✘	✘	Paragraph 5.4 and 5.5 of the	A regulated financial services business based in Mauritius or in an equivalent jurisdiction, provided that the Licensee	Simplified CDD

⁸³⁷Verification of identity is not required. Financial institution should obtain written declaration from other financial institution that holds documentary evidence of the existence of the legal entity and its regulated or listed status.

Annexure F, section F2.7.3.4					Code on the Prevention of Money Laundering and Terrorist Financing, 2012	is satisfied that the applicant for business is not acting on behalf of underlying principals. ⁸³⁸	
Mauritius Annexure F, section F2.7.3.4	✓	✗	✗	✗	Paragraph 5.4 and 5.5 of the Code on the Prevention of Money Laundering and Terrorist Financing, 2012	A public company listed on the Stock Exchange of Mauritius or on Recognised, Designated and Approved Stock/ Investment Exchanges or subsidiaries thereof. ⁸³⁹	Simplified CDD
Mauritius Annexure F, section F2.7.3.4	✓	✗	✗	✗	Paragraph 5.4 and 5.5 of the Code on the Prevention of Money Laundering and Terrorist Financing, 2012	Government administrations or enterprises and statutory bodies. ⁸⁴⁰	Simplified CDD
Mauritius Annexure F, section F2.7.3.4	✓	✓	✗	✗	Paragraph 5.4 and 5.5 of the Code on the Prevention of Money Laundering and	A pension, superannuation or similar scheme which provides retirement benefits to employees where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme. ⁸⁴¹	Simplified CDD

⁸³⁸ Licensees must obtain and retain documentary evidence of the financial services business and its regulated status.

⁸³⁹ Licensees must obtain a copy of the annual report and accounts of that public company and must verify that the individuals who purport to act on behalf of such entity have the necessary authority to do so. Licensees must also obtain and retain documentary evidence of the existence of the public company and of its listed status.

⁸⁴⁰ Licensees must obtain and retain documentary evidence of identification and verification of identity.

⁸⁴¹ In all transactions undertaken on behalf of an employer-sponsored scheme, Licensees must at a minimum identify and verify the identity of the employer and the trustees of the scheme (if any) as per the criteria set out in this Code.

					Terrorist Financing, 2012		
Mozambique See Annexure G, section G2.7.3.4	x	✓	x	✓	Article 10(2) (b)(i) and (ii) Law n° 14/2013	Financial institutions and non-financial bodies are required to identify their customers and confirm their identity through the presentation of valid documents every time they effect an occasional transactions of amounts equal to or above four hundred and fifty thousand meticaais (i) when the total amount of the transaction is not known at the time of commencement of the operation, the financial entity must proceed with the identification as soon as the amount is known and verify if the threshold has been reached and (ii) in case of a domestic or international transfer. ⁸⁴²	Proven Low Risk Exemption
Mozambique See Annexure G, section G2.7.3.4	x	✓	x	✓	Article 15(4)(c) Law n° 14/2013	Article 15(4)(c) also appears to be a an exemption as the law specifically states that the requirements as set out in Article 15 that pertain to electronic transfers are not applicable, "when it refers to transactions with a maximum limit of thirty thousand meticaais." ⁸⁴³	Proven Low Risk Exemption
Namibia See Annexure H, section H2.7.3.4	x	✓	x	✓	Section 2.1 of the General Exemption Order: Financial Intelligence Act, 2007, issued 5	For purposes of regulation 2(3) of the Regulations, an accountable institution is exempt from establishing the identity of a client concluding a single cash transaction, subject to the condition that such single cash transaction is less than or equal to the amount determined by the Financial Intelligence Centre under section 13(1) of the	Proven Low Risk Exemption

⁸⁴² The manner in which Article 10(1)(b) of Law n° 14/2013 is drafted appears to provide for a proven low risk exemption for both occasional transactions and domestic or international transfers below the threshold of 450, 000 Meticaais (USD 14197.97). While the threshold of USD/EUR 15,000 for occasional transactions is suggested in FATF Recommendation 10, Recommendation 10 only allows for a proven low risk exemption for wire transfers in the circumstances covered by Recommendation 16 and its interpretive note.

⁸⁴³ Thirty thousand meticaais is equivalent to USD 946.53 and while within the USD 1,000 de minimis threshold permitted by FATF Interpretive Note 16, paragraph 5 it is contradictory to the threshold listed in 10(1)(b) which applies to both domestic and international transfers. Article 15(4)(c) of Law n° 14/2013 is also in contravention of FATF Interpretive Note 16, paragraph 5 as the Mozambican provision states quite clearly that the provisions set out in Articles 15(1) to 15(3) are not applicable to transactions within the maximum limit of thirty thousand meticaais. This means that financial institutions do not have to ensure that they obtain originator and beneficiary information or that such information must accompany the transfer or that the information must accompany the relevant message over the course of the chain of payments, or that where an originator does not have a bank account, that one reference number must be attributed to the transaction. It therefore appears that the drafters of the new law have misunderstood that the flexibility permitted by the Interpretive Note to FATF Recommendation 16.

					May 2009 and paragraph 8(4) of Determination FICD 3	Act." It is hereby determined that such amount is five thousand Namibian dollars for any accountable institution under Schedule 1 of the Act, except an accountable institution under item 8, namely, a person who carries on the business of a casino or gambling institution, and twenty-five thousand Namibian dollars for any accountable institution under item 8 of Schedule 1 of the Act, namely, any person who carries on the business of a casino or gambling institution."	
Seychelles See Annexure I, section I2.7.3.4	x	✓	x	✓	Regulation 8(1) and 5 of the Anti-Money Laundering Regulations, 2012	Reporting entities are required to undertake CDD measures when: carrying out a one-off transaction. Regulation 5 defines a "once-off-transaction" as a transaction carried out other than as part of a business relationship that exceeds SCR100,000 or SCR50,000 in the case of cash transactions, whether the transaction is carried out in a single operation or several operations which appear to be linked."	Proven Low Risk Exemption
Seychelles See Annexure I, section I2.7.3.4	✓	✓	x	x	Regulation 11 of the Anti-Money Laundering Regulations, 2012	A reporting entity may apply customer due diligence measures in regulation 8(1)(a), (b) or (c) where – (a) the customer is – (i) a licensed bank; (ii) a recognized foreign bank; (iii) the Central Bank of Seychelles; (iv) a public body in Seychelles; or (b) there is reasonable grounds for believing that the product related to the relevant transaction is a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deductions from wages and the scheme rules do not permit the assignment of a member's interest under the scheme. ⁸⁴⁴	Discretionary CDD Simplified

⁸⁴⁴ The use of the word "may" in regulation 11(1) contrasted with the use of the word "shall" in regulation 11(2) provides discretion to reporting entities as to whether the CDD requirements set out in Regulation 8 need to be applied for specifically listed types of customers (licensed bank, recognized foreign bank, CBS or a public body in Seychelles) and products (pension, superannuation or similar scheme).

						(2) Where there is suspicion of money laundering, financing of terrorism or other criminal conduct, the reporting entity shall apply the customer due diligence measures in regulation 8(1)(a), (b) or (c)."	
South Africa See Annexure J, section J2.7.3.4	✓	✓	✗	✓	Exemption 17	Exemption 17 applies to Banks, Mutual Banks, the Post Bank, Ithala Development Finance Corporation and Domestic Money Remitters Business relationships (accounts and single transactions) Transaction limits – R5,000 per day, R25,000 per month. Only one account per institution and no cross border transfers ⁸⁴⁵	Simplified CDD Tiered CDD
South Africa See Annexure J, section J2.7.3.4	✓	✓	✗	✓	Banks Act Circular 6/2006 Cell Phone Banking	Circular 6 applies to cell-phone (mobile phone) banking product covered by exemption 17 Non-face-to-face account opening only regarded as adequate for low-value transactions – debits from accounts limited to R1,000 per day.	Simplified CDD Tiered CDD
South Africa See Annexure J, section J2.7.3.4	✓	✓	✗	✓	Gazette 33309 No. 560 Financial Intelligence Act (38/2011) Exemptions in Terms of the Act (2010) "Prepaid Instruments"	Prepaid Low Value Product Exemption Value of every transaction cannot exceed R200, available balance cannot exceed R1,500 at any time, monthly load limited to R3,000. Prepaid card can only be used domestically, cannot be used for domestic or cross-border remittances or to withdraw cash at an ATM or facilitate cash back.	Proven Low Risk Exemption
Swaziland See Annexure K, section K2.7.3.4	✗	✓	✗	✓	Section 7 Money Laundering and Financing of Terrorism (Prevention) Act 2011	CDD measures listed in sections 6(1), 6(2) and 6(3) do not apply in the following circumstances: if the transaction is an occasional transaction not exceeding two thousand, five hundred Emalangeni (E2,500) unless the accountable institution has reason to suspect that the transaction is suspicious or unusual.	Proven Low Risk Exemption

⁸⁴⁵Exemption 17.

Zimbabwe See Annexure N, section N2.7.3.3	✘	✔	✘	✔	Section 15(1)(b) Money Laundering and Proceeds of Crime Act, 2013 ⁸⁴⁶	Every financial institution and designated non-financial business or profession is required to identify each one of its customers and verify a customer's identity by means of an identity document when: when the customer, who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out a transaction in an amount equal to or exceeding five thousand United States dollars USD5,000 (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution), whether conducted as a single transaction or several transactions that appear to be linked, provided that the amount of the transaction is unknown at the time it is commenced, the customer's identification shall be verified as soon as the amount of the transaction has reached the prescribed amount.	Proven Low Risk Exemption
Zimbabwe See Annexure N, section N2.7.3.3	✘	✔	✘	✔	Section 15(1)(c) of the Money Laundering and Proceeds of Crime Act, 2013 ⁸⁴⁷	CDD is required when the customer, whether or not he or she is in an established business relationship with the financial institution, wishes to carry out a domestic or international wire transfer or monetary amounts in the amount equal to or exceeding one thousand United States dollars (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution. ⁸⁴⁸	Proven Low Risk Exemption

⁸⁴⁶ Act 4 of 2013.

⁸⁴⁷ Act 4 of 2013.

⁸⁴⁸ Section 15(1)(C).

9.2 Level of Compliance with Recommendation 11: Record Keeping

As represented in Table 68 below, all fourteen SADC countries have record keeping requirements set out in their national AML/CFT Law and or Regulations. The [FATF Recommendation 11](#) requires that documents should be kept for at least 5 years after the termination of a business relationship or after the date of an occasional transaction. SADC countries require records to be kept for a longer period of time, the longest period being 15 years in the case of Mozambique.⁸⁴⁹

Research has indicated that several countries laws and or regulations on a national level contain inconsistent time periods for which documents are to be kept, i.e. AML/CFT requirements conflict with the other relevant laws.

Most domestic AML/CFT laws and regulations require account files, business correspondence and the results of analysis undertaken to be kept for at least 5 years after the termination of the business relationship or the date of an occasional transaction. Lesotho is however the exception in this regard.

Whilst section 17(1)(b) of Lesotho's Money Laundering and Proceeds of Crime Act, 2008⁸⁵⁰ requires accountable institutions to keep a record of the nature of evidence obtained through the CDD process and to keep either a copy of the evidence or such information as would enable a copy to be obtained, section 17 of the of the Money Laundering and Proceeds of Crime Act, 2008 does not require accountable institutions to keep records for any other types of transactions. This is conflicted with section 39(2) of the Financial Institutions Act, 2012⁸⁵¹ which requires financial institutions to keep (a) accounting records, (b) financial statements, (c) records showing for each customer, at least on a daily basis, particulars of its transactions with or for the account of the customer, and the balance owing to or by each customer, (d) proper credit documentation, (e) large cash transactions, suspicious transactions and any other information relating to the combating of money laundering and terrorist financing, (f) customer or beneficiary identification data and business correspondence and (g) any other records as the Commissioner may determine.

South Africa is only one of two SADC countries to have issued exemptions with respect to the record keeping requirements. In South Africa, both Exemption 17 and the prepaid low value payment product exemption provide varying degrees of exemption from record keeping requirements. In terms of exemption 17, accountable institutions are only required to retain a copy of the client's identity document, which can be stored in hard copy or electronically, and keeping a record of the amount involved in the transaction, the parties to the transaction and all accounts that are involved in the transaction in the course of the business relationship or single transaction.⁸⁵² The prepaid low value payment product exemption on the other hand exempts prepaid low value payment product issuers from most record keeping obligations including the need to keep a copy of the clients ID. Issuers are however not exempted from keeping a record of the nature of that business relationship or transaction (section 22(1)(e)); in the case of a transaction the amount involved and the parties to that transaction (section 22(1)(f); all accounts that are involved in transactions concluded by that accountable institution in the course of that business relationship and a single transaction (section 22(1)(g).

⁸⁴⁹ Article 17 Law n° 14/2013.

⁸⁵⁰ Act 4 of 2008.

⁸⁵¹ Act 3 of 2012.

⁸⁵² PCC No. 21 on the Scope and Application of Exemption 17 in terms of FICA (As Amended).

Most SADC countries expressly permit documents to be kept in an electronic format. The exceptions are however the DRC, Mozambique, Swaziland and Zimbabwe. The DRC's Law n° 04/016 does not explicitly permit the keeping of records in electronic format. Mozambique's Law n° 14/2013 is silent on the manner in which records may be kept. Swaziland's Money Laundering and Financing of Terrorism (Prevention) Act, 2011 is not specific about the manner in which records are to be kept, save to say, that "where any record is required to be kept under this Act, a copy of it, with the appropriate back-up and recovery procedures, shall be kept in a manner as the Minister may by Regulations prescribe. To date, no regulations have been issued. Zimbabwe's Money Laundering and Proceeds of Crime Act, 2013⁸⁵³ and Bank Use Promotion and Suppression of Money Laundering Act, 2004 (As Amended)⁸⁵⁴ are also silent on the manner in which records should be kept.

It is interesting to note the approaches that have been taken by the Seychelles and Zambia in this regard. In Zambia, although Zambia's Financial Intelligence Centre Act, 2010⁸⁵⁵ is silent on the manner in which the records must be maintained, Directive 10(2) of the Bank of Zambia Anti-Money Directives 2004 requires regulated institutions to keep records by way of original documents in the form of hard copies or by using electronic storage devices. Records must be sufficient to permit a reconstruction of individual business transactions, including the amounts and types of currency involved, if any, so as to provide, if necessary, evidence for prosecution of criminal conduct.⁸⁵⁶ It is encouraging that Directive 10(2) makes use of the word "or" instead of the word 'and' in the wording 'to keep records by way of original documents in the form of hard copies or by using electronic storage devices', implying that hard copies of original documents do not need to be kept. Whilst the requirements related to the technical nature of the 'electronic storage device' are not specified in the Directive, Zambia has one of the most comprehensive *Electronic Communications and Transactions Acts* in the SADC region supported by the Electronic Communications and Transactions (General) Regulations.⁸⁵⁷ The Regulations cover *inter alia*: registration of cryptography service providers, accreditation of authentication service providers, technical requirements for authentication and certification and the protection of critical databases.

The Seychelles Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007 are particularly sensitive to the fact that reporting entities often 'find it necessary to rationalize their hard copy filing requirements' and that "most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements."⁸⁵⁸ As such, the Guidelines conform that retention may be by way of original documents or in a machine readable or electronic form as long as the paper copy can be readily reproduced from it. Paragraph 13.4 states further that "records kept in an electronic form must be kept in such a way that they can be authenticated. For these records to be acceptable or admissible in a court of law, a certification confirming the computer's reliability is likely to be required. The nature of that certificate and information that it must contain should be in accordance with recognised standards." It is unclear what standards are being referred to and by whom they are recognised.

⁸⁵³ Act 4 of 2013.

⁸⁵⁴ [Chapter 24:24].

⁸⁵⁵ Act 46 of 2010.

⁸⁵⁶ Directive 10(4) Bank of Zambia Anti-Money Directives 2004.

⁸⁵⁷ Electronic Communications and Transactions Act 21 of 2009 and Electronic Communications and Transactions (General) Regulations 2011.

⁸⁵⁸ Paragraph 13.3 of the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007.

Malawi is the only country in SADC that explicitly requires financial institutions to keep all records in soft copy **and** hardcopy. Regulation 17(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to keep all records in soft copy and hardcopy and ensure that appropriate back-up and recovery procedures are in place.

Table 68: Compliance with FATF Recommendation 11 – Record Keeping

Rec. 11 Record Keeping	Record Keeping Statutory Reference	FI's required to keep records for at least 5 years	Records obtained through CDD to be kept	Account files, business corresp. and the results of analysis undertaken to be kept for at least 5 years ⁸⁵⁹	Exemption to full record keeping req. has been issued	Docs may be kept in electronic format	Law explicitly requires a photocopy of ID documents be kept ⁸⁶⁰	The law requires CDD info. & trans. records to be made available to domestic competent authorities
Angola See Annexure A, section A2.7.4	Article 12 of Law n° 34/11	✓ (10 Yrs) ⁸⁶¹	✓	✓	✗	✓	✗	✓
Botswana See Annexure B, section B2.7.4	S11 to 15 Financial Intelligence Agency Act, 2009 ⁸⁶² , S16A(10) to 16A(13) Proceeds of Serious Crime Act, 1990 (As Amended) ⁸⁶³ and Regulations 12 and 13 Banking (Anti-Money Laundering)	✓ (5 Yrs)	✓	✓	✗	✓	✗	✓

⁸⁵⁹ Five years after the termination of the business relationship or the date of an occasional transaction.

⁸⁶⁰ Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification documents presented for verification purposes. It merely requires that the information and documents be stored and kept for five years.

⁸⁶¹ The requirement to keep records for a period of 10 years as set out in Article 12 of Law n° 34/11 is consistent with Article 150 of the Financial Institutions Law, Law n° 13/05 September 30 which applies to banking financial institutions and non-bank financial institutions. Article 40 of Law n° 5/05, the law of the National Payment System in Angola requires the retention of records by all "players of the payment system in electronic process or microfilming, for a period of five years from the date of issuance, if physical or by recording in their own computer system, if electronic, the payment instruments or records of payment electronic instructions." The five year timeframe in this law is however consistent with the timeframe set out in FATF Recommendation 11.

⁸⁶² Act 6 of 2009.

⁸⁶³ Act 19 of 1990.

	Regulations, 1995							
DRC See Annexure C, section C2.7.4	Article 12 of Law n° 04/016	✓ (10 Yrs)	✓	✓	✗	✗	✗	✓
Lesotho See Annexure D, section D2.7.4	S17(1)(a) Money Laundering and Proceeds of Crime Act, 2008 ⁸⁶⁴	✓ (5 Yrs)	✓	✗	✗	✓	✗	✓
Malawi See Annexure E, section E2.7.4	S27 Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁸⁶⁵ and Regulation 17 Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓ (7 Yrs) ⁸⁶⁶	✓	✓	✗	✓	✓	✓
Mauritius See Annexure F, section F2.7.4	S17(b) Financial Intelligence and Anti-Money Laundering Act, 2002 ⁸⁶⁷ ; Regulation 8 of the Financial Intelligence and Anti-Money Laundering Regulations, 2003 (As Amended)	✓ (5 Yrs)	✓	✓	✗	✓	✗	✓

⁸⁶⁴ Act 4 of 2008.

⁸⁶⁵ Act 11 of 2006.

⁸⁶⁶ This is consistent with paragraph 9.4.3 of the Reserve Bank of Malawi Guidelines for Mobile Payment Systems, 2011 that requires all settlement records to be retained for a minimum period of seven years.

⁸⁶⁷ Act 6 of 2002.

Mozambique See Annexure G, section G2.7.4	Article 17 Law nº 14/2013	✓ (15 Yrs)	✓	✓	✗	✗	✗	✓
Namibia See Annexure H, section H2.7.4	S26 Financial Intelligence Act 2012; ⁸⁶⁸ Exemption Order No. 75: General Exemptions: Financial Intelligence Act	✓ (5 Yrs)	✓	✓	✓ ⁸⁶⁹	✓	✗	✓
Seychelles See Annexure I, section I2.7.4	S6 Anti-Money Laundering Act, 2006 (As Amended) ⁸⁷⁰	✓ (7 Yrs)	✓	✓	✗	✓	✗	✓
RSA See Annexure J, section J2.7.4	S22 to 26 Financial Intelligence Centre Act, 2001 (As Amended) ⁸⁷¹	✓ (5 Yrs)	✓	✓	✓ ⁸⁷²	✓	✗	✓

⁸⁶⁸ Act 13 of 2012.

⁸⁶⁹ See Exemption Order No. 75: General Exemptions: Financial Intelligence Act.

⁸⁷⁰ Act 5 of 2006. In addition, see Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007.

⁸⁷¹ Act 38 of 2001 (As Amended).

⁸⁷² Both Exemption 17 and the prepaid low value payment product exemption provide varying degrees of exemption from record keeping requirements. In terms of exemption 17, accountable institutions are only required to retain a copy of the client's identity document, which can be stored in hard copy or electronically, and keeping a record of the amount involved in the transaction, the parties to the transaction and all accounts that are involved in the transaction in the course of the business relationship or single transaction. The prepaid low value payment product exemption on the other hand exempts prepaid low value payment product issuers from most record keeping obligations including the need to keep a copy of the clients ID. Issuers are however not exempted from keeping a record of the nature of that business relationship or transaction (section 22(1)(e)); in the case of a transaction the amount involved and the parties to that transaction (section 22(1)(f); all accounts that are involved in transactions concluded by that accountable institution in the course of that business relationship and a single transaction (section 22(1)(g).

<p>Swaziland</p> <p>See Annexure K, section K2.7.4</p>	<p>S8 Money Laundering and Financing of Terrorism (Prevention) Act 2011</p>	<p>✓ (5 Yrs)</p>	<p>✓</p>	<p>✓</p>	<p>✗</p>	<p>✗</p>	<p>✗</p>	<p>✓</p>
<p>Tanzania</p> <p>See Annexure L, section L2.7.4</p>	<p>S16 Anti-Money Laundering Act, 2006 (As Amended),⁸⁷³ Regulation 30 of the Anti-Money Laundering Regulations, 2012.</p>	<p>✓ (10 Yrs)</p>	<p>✓</p>	<p>✓</p>	<p>✗</p>	<p>✓</p>	<p>✗</p>	<p>✓</p>
<p>Zambia</p> <p>See Annexure M, section M2.7.4</p>	<p>S22 Financial Intelligence Centre Act, 2010⁸⁷⁴ and Directive 10 of the Anti-money Laundering Directives, 2004</p>	<p>✓ (10 Yrs)</p>	<p>✓</p>	<p>✓</p>	<p>✗</p>	<p>✓</p>	<p>✗</p>	<p>✓</p>
<p>Zimbabwe</p> <p>See Annexure N, section N2.7.4</p>	<p>S24 Money Laundering and Proceeds of Crime Act, 2013;⁸⁷⁵ S25 Bank Use Promotion and Suppression of Money Laundering Act, 2004 (As Amended)⁸⁷⁶</p>	<p>✓ (5 Yrs)</p>	<p>✓</p>	<p>✓</p>	<p>✗</p>	<p>✗</p>	<p>✗</p>	<p>✓</p>

⁸⁷³ Act 12 of 2006 (As Amended).

⁸⁷⁴ Act 46 of 2010.

⁸⁷⁵ Act 4 of 2013.

⁸⁷⁶ [Chapter 24:24].

9.3 Level of Compliance with Recommendation 13: Correspondent Banking

Regulations 19 and 21 of Malawi's Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 provide a very good example of how [FATF Recommendation 13](#) should be incorporated into domestic law and or regulation. It is recommended that other SADC countries consider Regulation 19 and 21 as the minimum harmonisation benchmark. Regulation 19 reads:

"19(1) In relation to correspondent banking and other similar business relationships, a financial institution shall, in accordance with these Regulations –

- (a) adequately identify and verify the correspondent institution or a respondent institution, whichever is applicable;
- (b) gather sufficient information about the nature of the business of the correspondent or respondent institution;
- (c) determine from publicly available information the reputation of the institution and the quality of supervision to which the correspondent or respondent institution is subject;
- (d) assess the adequacy and effectiveness of the anti-money laundering and terrorist financing controls of the correspondent or a respondent institution and document the findings;
- (e) obtain approval from senior management before entering a new correspondent or a respondent relationship;
- (f) obtain documents or agreements signed by senior management before establishing a new correspondent or a respondent relationship;
- (g) obtain certification from the correspondent or a respondent institution certifying that –
 - (i) in line with regulation 21(1), it carries out due diligence on other correspondent or respondent institutions it provides similar services; and
 - (ii) the correspondent or a respondent institution does not provide similar services to shell banks.

19(3) A financial institution shall take into consideration the risk posed by the jurisdiction in which a correspondent or respondent bank is located in considering entering into a relationship."

In addition, regulation 21 that prohibits financial institutions from entering into or continuing correspondent banking relationships with shall banks reads:

"21. A financial institution shall not enter into or continue correspondent banking relationships with a shell bank, or a respondent financial institution that permits their account to be used by shell banks."

The provisions found in AML/CFT laws and or regulations in Angola, Malawi, Mozambique Seychelles, Tanzania, Zambia and Zimbabwe with respect to correspondent banking are also compliant with FATF Recommendation 13. Of concern is the fact that correspondent banking is not covered at all in the legal and regulatory frameworks of Botswana and the DRC. This subject matter is also not covered in any guideline or guidance note. Additionally two SADC countries (Mauritius and South Africa) do not cover correspondent banking in law or regulation but have covered this topic in guidelines or guidance notes. It must be emphasised however that requirements found in guidance notes and guidelines are not requirements based in law, regulation or other enforceable means. Seven countries do not have legally enforceable provisions in law

or regulation prohibiting banks from entering into or continuing correspondent banking relationships with shell banks.

Table 69: Compliance with FATF Recommendation 13 – Correspondent Banking

	Statutory Reference	The AML/CFT Law & or Regulations contain a specific provision on correspondent banking	FIs are required by law to gather sufficient information about the respondent institution	FIs are required by law to assess the respondent institutions AML/CFT controls	FIs are required by law to obtain senior management approval when establishing a new correspondent banking relationship	Sending and receiving banks are required by law to understand the responsibilities of each institution	Law contains a provision on payable through accounts	Law or regulation prohibits institutions from entering into or continuing a relationship with shell banks
Angola See Annexure A, section A2.7.5	Article 23 of Law nº 34/11	✓	✓	✓	✓	✓	✓	✓
Botswana See Annexure B, section B2.7.5	NA	✗	✗	✗	✗	✗	✗	✗
DRC See Annexure C, section C2.7.5	NA	✗	✗	✗	✗	✗	✗	✗
Lesotho	S16(5) and 16(6) Money Laundering	✓	✓	✓	✓	✓	✓	✗

See Annexure D, section D2.7.5	and Proceeds of Crime Act, 2008 ⁸⁷⁷							
Malawi See Annexure E, section E2.7.5	S24(4), S24(6) and S24(7) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁸⁷⁸ Regulation 19 Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	✓	✓	✓	✓	✓	✓
Mauritius See Annexure F, section F2.7.5	Paragraphs 6.92 to 6.95 Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005	● ⁸⁷⁹	●	●	●	●	●	●
Mozambique See Annexure G, section G2.7.5	Article 10(8) and Article 14 Law n° 14/2013 Article 34(1) Law n° 14/2013	✓	✓	✓	✓	✓	✓	✓ ⁸⁸⁰

⁸⁷⁷ Act 4 of 2008.

⁸⁷⁸ Act 11 of 2006.

⁸⁷⁹ Provision found in a Guideline not in law or regulation.

⁸⁸⁰ Article 34(1) of Law n° 14/2013.

Namibia See Annexure H, section H2.7.5	Section 25 Financial Intelligence Act 2012 ⁸⁸¹	✓	✓	✓	✓	✓	✓	✗ ⁸⁸²
Seychelles See Annexure I, section I2.7.5	Regulations 14 and 17 Anti-Money Laundering Regulations, 2012	✓	✓	✓	✓	✓	✓	✓
RSA See Annexure J, section J2.7.5	Paragraph 28 Guidance Note 3 Guidance for Banks on Customer Identification and Verification and Related Matters, 2005	● ⁸⁸³	●	●	●	●	●	●
Swaziland See Annexure K, section K2.7.5	6(4) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓	✓	✓	✓	✓	✓	✗
Tanzania See Annexure L, section L2.7.5	Section C13 of the Schedule to the Anti- Money Laundering Regulations, 2012	✓	✓	✓	✓	✓	✓	✓

⁸⁸¹ Act 13 of 2012.

⁸⁸² The Financial Intelligence Act 2012 does not contain a provision on shell banks.

⁸⁸³ Measures that need to be put in place with respect to correspondent banking are not set out in the Financial Intelligence Centre Act, 2001 (As Amended) or Money Laundering and Terrorist Financing Control Regulations (MLTFCR). They are however covered in paragraph 28 of Guidance Note 3 Guidance for Banks on Customer Identification and Verification and Related Matters, 2005.

Zambia See Annexure M, section M2.7.5	Section 20 Financial Intelligence Centre Act, 2010 ⁸⁸⁴	✓	✓	✓	✓	✓	✓	✓
Zimbabwe See Annexure N, section N2.7.5	S14(2) and S21 Money Laundering and Proceeds of Crime Act, 2013 ⁸⁸⁵	✓	✓	✓	✓	✓	✓	✓

⁸⁸⁴ Act 46 of 2010.

⁸⁸⁵ Act 4 of 2013.

9.4 Level of Compliance with Recommendation 15: New Technologies

The new [FATF Recommendation 15](#) has only recently introduced the requirement that countries and financial institutions should identify and assess the money laundering and terrorist financing risks that may arise in relation to the development of new products, business practices and delivery mechanisms. FATF Recommendation 15 requires countries and financial institutions to identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms and (b) the use of new technologies for both new and pre-existing products. The recommendation also requires financial institutions to undertake risk assessments before the launch of new products, business practices or the use of new or developing technologies. Whilst FATF has not released an Interpretive Note for Recommendation 15, it has released a guidance paper on prepaid cards, mobile payments and Internet-based payment services.⁸⁸⁶ The paper refers to these innovative payment products and services as 'new payment products and services' (NPPS).⁸⁸⁷ The paper proposes guidance on the risk-based approach to AML/CFT measures and regulation in relation to NPPS of prepaid cards, mobile payments and Internet-based payment services, in line with the FATF Recommendations. The paper lists several risk factors associated with NPPS that include non-face-to-face relationships and anonymity, geographic reach, methods of funding, access to cash and the segmentation of services. It is important to note that Interpretative Note 10 also lists non-face-to-face business relationships or transactions as a potentially higher risk factor under the category product, service, transaction or delivery channel risk factors.

Despite Recommendation 15 being a new requirement, the AML/CFT Law and or Regulations in six SADC countries, namely Angola, Malawi, Namibia, Tanzania, Zambia and Zimbabwe contain provisions that require financial institutions to develop programmes that include policies and procedures to prevent the misuse of technological developments. The Law and or Regulation in seven countries require financial institutions to apply enhanced CDD measures for non-face-to-face account opening or transactions.

While it can be argued that the requirement to 'undertake a risk assessment prior to the launch of a new product, new business practice or the use of new or developing technologies' can conceivably be read into the requirement for financial institutions policies and procedures to prevent the misuse of technological development, none of the fourteen SADC countries expressly require accountable institutions to undertake a risk assessment prior to the launch of a new product, new business practice or the use of new or developing technologies.

⁸⁸⁶ See Financial Action Task Force (FATF) *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services 4* where the following is stated, "For the purposes of this guidance, NPPS are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations."

⁸⁸⁷
3.

Table 70: Compliance with Recommendation 15

Rec. 15 New Technologies	A: Financial institutions are required by the AML/CFT Law or Regulation to identify and assess the ML/TF risks that may arise in relation to the development of new products	B: The AML/CFT Law or Regulation requires enhanced CDD for non-face-to-face account opening / transactions	C: The AML/CFT Law or Regulation requires financial institutions to undertake a risk assessment prior to the launch of a new product, new business practice or the use of new or developing technologies
Angola See Annexure A, section A2.7.7	✓ Article 8(3) of Law n° 34/11	✓ Article 10(3) of Law n° 34/11 ⁸⁸⁸	✗
Botswana See Annexure B, section B2.7.7	✗	✗	✗
DRC See Annexure C, section C2.7.7	✗	✗	✗
Lesotho See Annexure D, section D2.7.7	✗	✗	✗

⁸⁸⁸ Article 10(3) specifically relates to non-face-to-face transactions and reads “enhanced due diligence measures shall always be applicable to non-face to face transactions, especially to those that may favor the anonymity, operations carried out with Politically Exposed Persons, correspondent banking transactions with financial banking institutions incorporated in third countries, as well as to other operations as may be designated by the supervisory or inspection authorities of the respective sector, provided that they are legally endowed to this effect.”

Malawi See Annexure E, section E2.7.7	✓ ⁸⁸⁹ Regulation 23 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	x	x
Mauritius See Annexure F, section F2.7.7	x	x	x
Mozambique See Annexure G, section G2.7.7	x	✓ Article 10(2)(e) of Law n° 14/2013	x
Namibia See Annexure H, section H2.7.7	✓ ⁸⁹⁰ S39 Financial Intelligence Act 2012 ⁸⁹¹	✓ S39 Financial Intelligence Act 2012	x

⁸⁸⁹ Regulation 23 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to “take reasonable steps to prevent the use of new technologies for money laundering or terrorist financing schemes” but no guidelines or PCCs have been issued by the FIU to help financial institutions to understand what “reasonable steps” might be. There are no obligations set out in law for accountable institutions to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

⁸⁹⁰ Section 39 of the Financial Intelligence Act 2012 deals with internal controls and specifically requires accountable and reporting institutions to, “develop, adopt and implement a customer acceptance policy, internal rules, programmes, policies, procedures and controls as prescribed to effectively manage and mitigate risks of ML/TF. Section 39(5) of the Financial Intelligence Act 2012 states clearly that programmes must include: policies and procedures to prevent the misuse of technological developments, including those related to electronic means of storing and transferring funds or value; policies and procedures to address the risks associated with non-face-to-face clients or transactions for the purposes of identifying and on-going customer due diligence.

⁸⁹¹ Act 13 of 2012.

Seychelles See Annexure I, section I2.7.7	x	x	x
RSA See Annexure J, section J2.7.7	x ⁸⁹²	✓ ⁸⁹³ Regulation 18 of the Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended)	x
Swaziland See Annexure K, section K2.7.7	x	x	x
Tanzania See Annexure L, section L2.7.7	✓ ⁸⁹⁴ Section C6 of the Schedule to the Anti-Money Laundering Regulations, 2012	✓ Section C6 of the Schedule to the Anti-Money Laundering Regulations, 2012	x

⁸⁹² The Financial Intelligence Centre Act, 2001 (As Amended) does not address the need for accountable institutions to have policies in place to address the potential abuse of new technological developments for money laundering or terrorist financing.

⁸⁹³ Regulation 18 of the Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended) applies to the non-face-to-face transactions and requires accountable institutions that obtained information about a natural or legal person, partnership or trust without contact in person with that natural person, or with a representative of that legal person or trust, to take reasonable steps to establish the existence or to establish or verify the identity of that natural or legal person, partnership or trust.

⁸⁹⁴ Section C6 of the Schedule to the Anti-Money Laundering Regulations, 2012 specifically requires banks or financial institution to pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and to take measures, if needed, to prevent their use in money laundering schemes. Banks and or financial institutions are also required to have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.

Zambia	✓ ⁸⁹⁵	✓ ⁸⁹⁷	✗
See Annexure M, section M2.7.7	S32 Financial Intelligence Centre Act, 2010 ⁸⁹⁶	S18 Financial Intelligence Centre Act, 2010; Directive 6(4) of the Bank of Zambia Anti-Money Directives, 2004	
Zimbabwe	✓	✓ ⁸⁹⁹	✗
See Annexure N, section N2.7.7	S25 Money Laundering and Proceeds of Crime Act, 2013 ⁸⁹⁸	S19 Money Laundering and Proceeds of Crime Act,	

⁸⁹⁵ Section 32 Financial Intelligence Centre Act, 2010, which deals with internal controls, specifically requires reporting entities in Zambia to develop and implement programmes for the prevention of money laundering, financing of terrorism and any other serious offence. Such programmes must include policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value. Whilst this provision is contained in the Act, no guidance has been published on what these policies and procedures should contain.

⁸⁹⁶ Act 46 of 2010.

⁸⁹⁷ . Section 18 of the Financial Intelligence Centre Act, 2010 requires reporting entities where conducting any business relationship or executing transactions with a customer that is not physically present for the purposes of identification, to take adequate measures to address the specific risk of money laundering, financing of terrorism and any other serious offence. Importantly, reporting entities must ensure that the CDD conducted is no less effective than where the customer appears in person. In addition, reporting entities are required to obtain additional documentary evidence or supplementary measures to verify or certify the documents supplied by the customer, or confirmatory certification from financial institutions or other documentary evidence or measures as may be prescribed. As far as can be determined, no such additional requirements have been prescribed. Directive 6(4) of the Bank of Zambia Anti-Money Directives, 2004 also requires regulated institutions to establish clear procedures on how to identify a customer who applies to open an account through the internet or other electronic means. Regulated institutions are further not permitted to establish a business relationship through this means unless the identity documents of the customer have been verified or confirmed. No additional guidance is provided on how regulated institutions can meet their obligations under this Directive.

⁸⁹⁸ Act 4 of 2013.

⁸⁹⁹ section 19 of the Money Laundering and Proceeds of Crime Act, 2013 which deals with situations where customers are not physically present (non-face-to-face) transactions, requires financial institutions and designated non-financial businesses and professions to take adequate measures to address the specific risk of money laundering and financing of terrorism in the event they conduct business relationships or execute transactions with a customer who is not physically present for purposes of identification. Importantly, they are required to ensure that CDD measures are no less effective than where the customer appears in person. The section states further that non-face-to-face transactions “may require additional documentary evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory confirmation from financial institutions or other documentary evidence or measures, as may be prescribed in directives.” No directives have been issued on this subject.

9.5 Level of Compliance with Recommendation 16: Wire Transfers

In the recent ESAAMLG report on financial inclusion it is noted that, “none of the countries that participated in the survey allow simplified CDD [or a proven low risk exemption] for cross-border financial services. Given the current levels of cross-border money flows in the ESAAMLG region and the objectives of increased integration, it is worth considering whether general frameworks for simplified CDD in relation to cross-border financial services should be developed. This is a matter that national regulators should consider jointly. Frameworks may provide simply for communication between relevant regulators when providers approach a regulator in on country with a proposed product or service. They may also extend to a more detailed tiered system that would enable providers to develop a range of different products within different risk-based parameters set by regulators jointly for such services in the region.”⁹⁰⁰

An important update on this report is that Zimbabwe who was a participant in the survey and has since included the *de minimis* exemption of US\$1,000 in section 27 of the Money Laundering and Proceeds of Crime Act, 2013.⁹⁰¹ The survey was however conducted before the new Act was passed.

The scope, ambit and implications of the *de minimis* threshold as reformulated in FATF Recommendation 16 is succinctly summarised by the European Commission DG Internal Market and Services (DG MARKT) as follows:

“The *de-minimis* threshold of USD/EUR 1,000 has been retained in the new Recommendation; however, the new Recommendation spells out clearly what information is still required for international wire transfers under this threshold. This includes the names of the originator and the beneficiary as well as the account number of both parties. The latter can be replaced by a unique transaction reference number. The address/national ID number/customer ID number/date and place of birth are no longer required. The accuracy of the information need only be verified in the case of suspicion of money laundering.”⁹⁰²

The manner in which the *de minimis* threshold has been included in two AML Laws passed by SADC Member States post the release of the revised FATF Recommendations provides insight into how countries have chosen to interpret the flexibility provided by [FATF Recommendation 16](#).

Section 27 of the Zimbabwean Money Laundering and Proceeds of Crime Act, 2013⁹⁰³ reads:

‘When undertaking wire transfers equal to or exceeding **one thousand United States dollars** financial institutions (or such lesser or greater amount as may be prescribed), shall –

- (a) identify and verify the identity of the originator;

⁹⁰⁰ Alliance for Financial Inclusion / Eastern and Southern Africa Anti-Money Laundering Group *Public and Private Sector Survey Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices* 29.

Twelve countries, namely, Botswana, Comoros, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Zambia and Zimbabwe participated in the survey.

⁹⁰¹ Act 4 of 2013.

⁹⁰² European Commission DG Internal Market and Services (DG MARKT) *Additional Research to Assess the Impact of Potentially Changing the Scope (Art. 3) of the Regulation on Information Accompanying Transfers of Funds* 14.

⁹⁰³ Act 4 of 2013.

- (b) obtain and maintain the account number of the originator or, in the absence of an account number, a unique reference number;
- (c) obtain and maintain the originator's address or, in the absence of an address, the originator's national identity number or date and place of birth; and
- (d) include information referred to in paragraphs (a), (b) and (c) in the message or payment form accompanying the transfer.'

Financial institutions are not required to verify the identity of a customer with which it has an existing business relationship, provided that it is satisfied that it already knows and has verified the true identity of the customer.⁹⁰⁴ Section 27(4) of the Money Laundering and Proceeds of Crime Act, 2013 states that 'a directive may modify the requirements set forth in subsection (1) –

- (a) with respect to domestic wire transfers, as long as the directive provides for full originator information to be made available to the beneficiary financial institution and appropriate authorities by other means; and
- (b) with regard to cross-border transfers where individual transfers from a single originator are bundled in a batch file, as long as the directive provides for the originator's account number or unique reference number to be included, and that the batch file contains full originator information that is full traceable in the recipient country.'

Financial institutions that receive wire transfers that do not contain the complete originator information required must take measures to obtain and verify the missing information from the ordering institution or the beneficiary.⁹⁰⁵ In the event that the financial institution is unable to obtain any missing information, it is required to refuse acceptance of the transfer and report it to the unit.⁹⁰⁶

The Zimbabwean interpretation of Recommendation 16 is interesting in that section 27 of the Money Laundering and Proceeds of Crime Act, 2013 includes the de minimis threshold of USD1,000 but the manner in which section 27 is drafted seems to imply that all wire transfers, be they domestic or cross-border transfers, occasional or regular, that are below the USD1,000 threshold are exempt from the requirements set out in sections 27(1)(a) – (d). This is not the intention behind the exemption for occasional cross-border wire transfers as set out in the Interpretive Note to Recommendation 16.

A similar problem is evident in the drafting of Article 15 of Mozambique's Law n° 14/2013 that reads:

1. Financial institutions, including those dedicated to the transfer of funds, must ensure they obtain and confirm exact and useful information in respect of the originator and beneficiary, of the funds transferred and messages concerning them.
2. The information referred to in the previous number must accompany the transfer or the relevant message, over the course of the chain of payments.
3. If the originator does not have a bank account, the financial institutions, including those dedicated to the transfer of funds, must maintain a thorough vigilance and an adequate control, with a view to detect any

⁹⁰⁴ Section 27(2) of Act 4 of 2013.

⁹⁰⁵ Section 27(6).

⁹⁰⁶ Section 27(7).

suspicious activities and transfers of funds without complete information on the originator or beneficiary and attribute only one reference number to the transactions, to permit tracking of the operation.

4. The provisions contained in the previous numbers are not applicable in the following instances:
 - (a) When the transaction is effected using a credit card or debit or pre-paid for the purchase of goods and services, if the transaction effected is linked to the identification number of the card;
 - (b) When it refers to transactions effected between financial institutions and respective regularizations, and both the originator and the beneficiary act on their own behalf;
 - (c) When it refers to transactions within the maximum limit of thirty thousand meticaís.”

While the thirty thousand meticaís set in Article 15(4)(c) is equivalent to USD 946.53 and within the USD 1,000 de minimis threshold permitted by FATF Interpretive Note 16, paragraph 5 it is contradictory to the threshold listed in Article 10(1)(b) of Law n° 14/2013 that applies to both domestic and international transfers. Article 15(4)(c) of Law n° 14/2013 also appears to be in contravention of FATF Interpretive Note 16, paragraph 5 as the Mozambican provision states quite clearly that the provisions set out in Articles 15(1) to 15(3) are not applicable to transactions within the maximum limit of thirty thousand meticaís. This means that financial institutions do not have to ensure that they obtain originator and beneficiary information or that such information must accompany the transfer⁹⁰⁷ or that the information must accompany the relevant message over the course of the chain of payments,⁹⁰⁸ or that where an originator does not have a bank account, that one reference number must be attributed to the transaction.⁹⁰⁹ It therefore appears that the drafters of the new law have misunderstood the flexibility permitted by the Interpretive Note to FATF Recommendation 16 which allows countries to permit financial institutions not to have to **verify** the name of the originator, the name of the beneficiary and the account number for each or a unique transaction number for occasional cross-border wire transfers below the threshold of USD1, 000.⁹¹⁰ This information should however still be provided.

Table 71 below provides a summary of each countries level of compliance with FATF Recommendation 16. It is important to note that three countries (Botswana, Mauritius and Tanzania) do not make any reference to wire transfers or electronic funds transfers in their primary AML Laws. The DRC Law n° 04/016 does not contain a specific provision on wire transfers but Article 6 requires all transfer of funds and securities to and from abroad for an amount equal or in excess of 10,000 USD to be done through a credit institution. The Seychelles does contain a provision on electronic funds transfer, but no distinction is made between domestic and cross-border transfers.

⁹⁰⁷ Article 15(1) Law n° 14/2013.

⁹⁰⁸ See Article 15(2).

⁹⁰⁹ See Article 15(2).

⁹¹⁰ Interpretive Note 16 paragraph 5 states, “Countries may adopt a de minimis threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply: (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer; (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.”

Table 71: Compliance with FATF Recommendation 16

Rec. 16 Wire Transfers	AML/CFT Act contains a provision on cross-border and domestic wire transfers	AML/CFT Regulation contains a provision on cross-border and domestic wire transfers	The law refers to electronic funds transfer instead of wire transfer	Law requires accurate originator and beneficiary information to accompany qualifying cross-border wire transfers ⁹¹¹	Where FI identifies incomplete information of sender, it is required to reject the transfer or request additional information and or report such to the FIU	De minimis threshold for cross-border wire transfer (no higher than US\$1,000) contained in Law or Regulation
Angola See Annexure A, section A2.7.8	✓ Article 27 Law n° 34/11	✗	✗	✓ ⁹¹² Article 27 Law n° 34/11	✓ ⁹¹³ Article 27(9) Law n° 34/11	✗
Botswana See Annexure B, section B2.7.8	✗	✗	✗	✗	✗	✗

⁹¹¹ The Law requires the name of originator, originators account number, address, or national identity number, or customer identification number, or date and place of birth, name of beneficiary and beneficiary account number to accompany all qualifying cross-border wire transfers.

⁹¹² Article 27 Angola's Law n° 34/11 is directly applicable to wire transfers. Financial institutions conducting wire transfers are required to include in the message or on the payment form accompanying the transfer a) the [senders] full name, b) account number, c) address and d) where necessary, the name of the financial entity of the sender. Article 27(2) allows for the address to be replaced by the date and place of birth of the sender, his identity card number or by the client identification number. In addition, where there is no account number, Article 27(3) allows for the transfer to be accompanied by a single reference number that facilitates the tracking of the transaction to its sender. Where the wire transfer is a domestic transfer (sender and recipient both being located in Angola, the only information which must accompany the transfer is the account number or single reference number that enables the tracking of the wire transfer to its sender. This waiver of required information is however only applicable where the financial entity of the sender is able to make available additional information on the sender, within three working days, from the date of reception of the request from the financial entity of the beneficiary, or other competent authorities. Financial institutions that act as intermediaries in the payment chain are required to collect all the information accompanying the transfer and transmit it to the next financial institution in the payment chain.

⁹¹³ Recipient financial institutions are required to adopt risk-based measures to confirm the completeness of the information on the transfer sender and where the financial entity of the beneficiary identifies the existence of incomplete information of the sender, it is required to reject the transfer or request the financial entity of the sender to send full information on the sender.

DRC See Annexure C, section C2.7.8	✗ ⁹¹⁴	✗	✗	✗	✗	✗
Lesotho See Annexure D, section D2.7.8	✓ S22(1) Money Laundering and Proceeds of Crime Act, 2008 ⁹¹⁵	✗	✓	✓ ⁹¹⁶ S22(1) Money Laundering and Proceeds of Crime Act, 2008	✗	✗
Malawi See Annexure E, section E2.7.8	✓ S33 Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁹¹⁷	✓ Regulation 18 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	✓ Regulation 18 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓ Regulations 19(4) and 19(5) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✗
Mauritius	✗	✗	✗	● ⁹¹⁸	●	✗

⁹¹⁴Law n° 04/016 does not contain a specific provision on wire transfers but Article 6 requires all transfer of funds and securities to and from abroad for an amount equal or in excess of 10,000 USD to be done through a credit institution.

⁹¹⁵ Act 4 of 2008.

⁹¹⁶ Section 22(1) of the Money Laundering and Proceeds of Crime Act, 2008 refers to “accurate originator information” but does not provide details on what is to be included.

⁹¹⁷ Act 11 of 2006. Section 33 does not distinguish between cross-border and domestic transfers.

⁹¹⁸ Wire transfers are not covered in either the Financial Intelligence and Anti-Money Laundering Act, 2002 or the Financial Intelligence and Anti-Money Laundering Regulation, 2003 (As Amended). Paragraph 6.109 of the Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005 however provides guidance on this subject. This paragraph reads, “to ensure that wire transfer systems are not used by criminals as a means to break the audit trail, where a financial institution makes a payment on behalf of its customer, accurate and meaningful originator information (name, residential address and any account number or reference of the originator) should be included on all funds transfers and related messages and should remain with the transfer through the payment chain until it reaches its final destination. This information is particularly important for international transfers on behalf of individual customers to ensure that the source of funds can be identified in the event of an

See Annexure F, section F2.7.8				Paragraph 6.109 Guidance Notes on AML/CFT for Financial Institutions, 2005		
Mozambique See Annexure G, section G2.7.8	✓ Article 15 Law n° 14/2013	✗	✓	✓ Article 15 of the Mozambican Law n° 14/2013	✗	✓ Article 15(4)(c) of the Mozambican Law n° 14/2013
Namibia See Annexure H, section H2.7.8	✓ S34 Financial Intelligence Act 2012 ⁹¹⁹	✓ Determination BID-3 ⁹²⁰	✓	✓ S34(2) Financial Intelligence Act 2012	✓ S34(4), 34(5) and 34(6) Financial Intelligence Act 2012	✓ ⁹²¹
Seychelles See Annexure I, section I2.7.8	✓ S 8(1) Anti-Money Laundering Act, 2006 (As Amended) ⁹²²	✗ ⁹²³	✓	✓ S 8(1) Anti-Money Laundering Act, 2006 (As Amended) ⁹²⁴	✗	✗
RSA	✓ ⁹²⁵	✗	✓	✗	✗	✗

investigation in the receiving jurisdiction.” Financial institutions are also required to conduct enhanced scrutiny of, and monitor for suspicious activity and incoming funds transfers that do not contain complete originator information.

⁹¹⁹ Act 13 of 2012.

⁹²⁰ Determination BID-3 on Money Laundering and “Know Your Customer” Policy contains a general provision on “funds transfer”.

⁹²¹ Neither the Financial Intelligence Act 13 of 2012 or Determination BID-3 on Money Laundering and “Know Your Customer” Policy contain the suggested an explicit de minimus threshold of US\$1,000 for cross-border wire transfers (electronic transfers), although the wording “funds in excess of a prescribed amount” provides room for the Regulator to prescribe a de minimus threshold of US\$1,000 in the future.

⁹²² Act 5 of 2006.

⁹²³ The Anti-Money Laundering Regulations, 2012 make no reference to wire transfers or electronic funds transfers.

⁹²⁴ No distinction is made between domestic and cross-border transfers.

See Annexure J, section J2.7.8	S31 Financial Intelligence Centre Act, 2001 (As Amended) ⁹²⁶					
Swaziland See Annexure K, section K2.7.8	✓ ⁹²⁷ S10(1) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✗	✓	✓ S 10(1) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓ S11(1) and 11(2) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✗
Tanzania See Annexure L, section L2.7.8	✗ ⁹²⁸	✗	✗	✗	✗	✗
Zambia See Annexure M, section M2.7.8	✓ S26 of the Financial Intelligence Centre Act, 2010 ⁹²⁹	✗	✗	✓ S26(1) Financial Intelligence Centre Act, 2010	✓ S26(6) and 26(7) Financial Intelligence Centre Act, 2010	✓ ⁹³⁰ S26(1) Financial Intelligence Centre

⁹²⁵ Section 31 of the Financial Intelligence Centre Act, 2001 (As Amended) only deals with reporting requirements and is largely non-compliant with FATF Recommendation 16.

⁹²⁶ Act 38 of 2001 (As Amended).

⁹²⁷ Section 10(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 applies both to financial institutions and money transmission service providers and requires these accountable institutions to include accurate originator information and other related messages with electronic funds transfers and such information shall remain with the transfer. This does not apply to electronic funds transfers and settlements between financial institutions where the originator and beneficiary of the funds transfers are acting on their own behalf. As no regulations have been issued under the Money Laundering and Financing of Terrorism (Prevention) Act 2011, no details are provided with respect to the content of the "accurate originator information and other related messages." The provision does also not distinguish between the information required for domestic versus cross-border wire transfers.

⁹²⁸ Requirements with respect to wire transfers are not set out in the Anti-Money Laundering Act 12 of 2006 (As Amended) or the Anti-Money Laundering Regulations, 2012.

⁹²⁹ Act 46 of 2010.

						Act, 2010
Zimbabwe See Annexure N, section N2.7.8	✓ S27 Money Laundering and Proceeds of Crime Act, 2013 ⁹³¹	✗	✗	✓ S27(1) Money Laundering and Proceeds of Crime Act, 2013	✓ S27(6) and 27(7) Money Laundering and Proceeds of Crime Act, 2013	✓ S27 Money Laundering and Proceeds of Crime Act, 2013

⁹³⁰ Financial institutions undertaking any wire transfers equal to, or above, such amounts as may be prescribed are required to: identify and verify the identity of the originator; obtain and maintain the account number of the originator, or in the absence of an account number, a unique reference number; obtain and maintain the originator's address or, in the absence of address, the national identity number, or date and place of birth; and include information listed above in the message or payment form accompanying the transfer." As is the case with respect to several provisions in the Financial Intelligence Centre Act, 2010 that contain the words "as may be prescribed" or "as prescribed by the Minister", nothing has been prescribed with respect to the thresholds applicable to wire transfers, implying (on a matter of interpretation) that either all wire transfers must contain the details set out above or none require this information. It may have been the intention of the drafters of the law to make future provision for the flexibility allowed by FATF Recommendation 16 with respect to the application of the permitted de minimis threshold.

⁹³¹ Act 4 of 2013.

9.6 Level of Compliance with Recommendation 17: Reliance on Third Parties

Most SADC Member States' AML/CFT Laws and or Regulations contain provisions permitting financial institutions to rely on third parties to perform several CDD measures and introduce business [FATF Recommendation 17]. Notable exceptions are Botswana, DRC, Mozambique, South Africa and Tanzania. In Botswana, section 13 of the Financial Intelligence Agency Act, 2009⁹³² allows for record keeping obligations set out in section 11 of the Act to be performed by a third party but the Financial Intelligence Agency Act, 2009 is silent on CDD obligations being undertaken by third parties. The DRC Law n° 04/016 does not contain any provisions related to reliance on third parties. In South Africa, the only reference made to reliance on third parties in the Financial Intelligence Centre Act, 2001 (As Amended)⁹³³ is with respect to an accountable institution's record keeping obligations (section 22). The Financial Intelligence Centre Act, 2001 (As Amended) does not contain any provisions permitting accountable institutions to outsource CDD requirements to third parties. PCC12 Outsourcing of Compliance Activities to Third Parties which was issued by FIC in 2012 however clear states, "An accountable institution may utilise the services of a third party to perform activities relating to the establishing and verifying of clients' identities as well as the collection of required documents to establish and verify the identity of their clients, and for record-keeping purposes as required in terms of the FIC Act and the Regulations to the FIC Act. However, an accountable institution remains liable for compliance failures associated with and/or caused by such an outsourcing arrangement. In terms of Exemption 5 to the Financial Intelligence Centre Act, 2001 (As Amended), every accountable institution is exempted from compliance with the provisions of Section 21 of the Act which require the verification of the identity of a client of that institution if: a) that client is situated in a country where, to the satisfaction of the relevant supervisory body, anti-money laundering regulation and supervision of compliance with anti-money laundering regulation, which is equivalent to that which applies to the accountable institution is in force, b) a person or institution in that country, which is subject to the antimoney laundering regulation referred to in paragraph (a) confirms in writing to the satisfaction of the accountable institution that the person or institution has verified the particulars concerning that client which the accountable institution has obtained in accordance with Section 21 of the Act, and c) the person or institution referred to in paragraph (b) undertake to forward all documents obtained in the course of verifying such particulars to the accountable institution.

⁹³² Act 6 of 2009.

⁹³³ Act 38 of 2001 (As Amended).

Table 72: Compliance with FATF Recommendation 17

Rec. 17 Reliance on Third Parties	AML/CFT Law or Regulation permits financial institutions to rely on third parties to perform several CDD measures	Third parties are required by Law or Regulation to make available to the financial institution copies of identification data and other documentation upon request and without delay	Financial institution is required by Law or Regulation to satisfy itself that the third party is regulated, supervised and has measures in place to meet CDD and record keeping requirements
Angola See Annexure A, section A2.7.9	✓ ⁹³⁴ Article 22 of Law n° 34/11	✗	✗
Botswana See Annexure B, section B2.7.9	● ⁹³⁵	✗	✗
DRC See Annexure C, section C2.7.9	✗	✗	✗
Lesotho See Annexure D, section	✓ S16(7) Money Laundering and Proceeds of Crime Act, 2008 ⁹³⁶	✓ S16(7)(a) and (b) Money Laundering and Proceeds of Crime Act, 2008	✓ ⁹³⁷ S16(7)(c) Money Laundering and Proceeds of Crime Act,

⁹³⁴ Article 22 of Law 34/11 provides for financial institutions, with the exclusion of exchange offices and money transfer companies, to be allowed to have part of their CDD process to be performed by third parties, but only after issuance of implementing regulations by the competent supervisory authorities, which has not occurred (ESAAMLG 2012).

⁹³⁵ Section 13 of the Financial Intelligence Agency Act 6 of 2009 allows for the record keeping obligations set out in section 11 of the Act to be performed by a third party on behalf of the specified party. Specified parties must provide the Financial Intelligence Agency with the particulars of the third party as may be prescribed. Section 13(3) places the liability for non-performance of the obligations imposed by section 11 by the third party with the specified party. The Act is however silent on CDD obligations being undertaken by third-parties.

⁹³⁶ Act 4 of 2008.

⁹³⁷ An accountable institution is also required to ensure that the third party or intermediary is regulated and supervised and has the requisite measures in place to comply with the requirements as set out in the Act. The Money Laundering and

D2.7.9			2008
Malawi See Annexure E, section E2.7.9	✓ S24(6) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006; ⁹³⁸ Regulation 20(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓ S24(6)(a) and (b) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006	✓ S24(6)(c) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006
Mauritius See Annexure F, section F2.7.9	✓ Regulation 4(6) of the Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓ Regulation 4(6) of the Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓ Regulation 4(6) of the Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)
Mozambique See Annexure G, section G2.7.9	✗	✗	✗
Namibia See Annexure H, section H2.7.9	✓ ⁹³⁹ S29 Financial Intelligence Act 2012 ⁹⁴⁰ General Exemptions (paragraphs 2.2. to 2.4)	✓ General Exemptions (paragraphs 2.2. to 2.4)	✓ General Exemptions (paragraphs 2.2. to 2.4)

Proceeds of Crime Act 4 of 2008 falls short however with respect to there being no provision for making accountable institutions ultimately responsible / liable for the actions of intermediaries or third parties.

⁹³⁸ Act 11 of 2006.

⁹³⁹ The only reference made to reliance on third parties in the Financial Intelligence Act 13 of 2012 is with respect to an accountable institution's record keeping obligations (section 29). In terms of section 29 accountable or reporting institutions are permitted to rely on third parties to perform the record keeping duties imposed by section 26, provided that the accountable or reporting institution has unrestricted access to the records. As per section 29(2), if a third party fails to comply with the reporting requirements set out in section 26 of the Act, the accountable or reporting institution is liable for the failure. If an accountable or reporting institution appoints a third party to perform the reporting duties imposed by section 26, the accountable or reporting institution is required to provide the Centre with the prescribed particulars regarding the third party.

The Financial Intelligence Act 2012 does not contain any provisions specifically related to the reliance on third parties to undertake the CDD measures set out in Recommendation 10 (a) to (c).

⁹⁴⁰ Act 13 of 2012.

Seychelles See Annexure I, section I2.7.9	✓ ⁹⁴¹ Regulation 12 Anti-Money Laundering Regulations, 2012	✓ Regulation 12 of the Anti-Money Laundering Regulations, 2012	✓ Regulation 12 of the Anti-Money Laundering Regulations, 2012
RSA See Annexure J, section J2.7.9	✓ ⁹⁴² Exemption 5	✓ Exemption 5	✓ Exemption 5
Swaziland See Annexure K, section K2.7.9	✓ S6(6) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓ S6(6)(a) and (b) Money Laundering and Financing of Terrorism (Prevention) Act 2011	✓ S6(6)(c) Money Laundering and Financing of Terrorism (Prevention) Act 2011
Tanzania See Annexure L, section L2.7.9	✓ Regulation 31(2) of the Anti-Money Laundering Regulations, 2012	✓ Regulation 31(2) of the Anti-Money Laundering Regulations, 2012	✗
Zambia See Annexure M, section M2.7.9	✓ S17(1) Financial Intelligence Centre Act, 2010 ⁹⁴³	✓ S17(1)(b) and (c) Financial Intelligence Centre Act, 2010	✓ S17(1) (c) Financial Intelligence Centre Act, 2010
Zimbabwe See Annexure	✓ S18 Money Laundering and	✓ Section 18(1)(c) Money	✓ Section 18(1)(c) Money

⁹⁴¹ It is important to note that Regulation 12 of the Anti-Money Laundering Regulations, 2012 does not apply to licensed banks, bureau de change and persons who by way of business provide the following services to third parties (a) acceptance of deposits and other repayable funds from the public and (b) lending, including customer credit, mortgage credit, factoring, financing of commercial transactions, including forfeiting. This implies that these entities are required to undertake CDD measures themselves and may not rely on third parties to do so.

⁹⁴² Exemption 5 provides that a South African institution may, for verification purposes, rely on a confirmation of a customer's identity by a regulated institution in a foreign jurisdiction. This applies where a foreign customer engages directly with a South African institution and the South African institution is assisted in the verification process by obtaining confirmation of the customer's identity from a foreign institution. It is important to note however that this exemption is only applicable to foreign customers.

⁹⁴³ Act 46 of 2010.

N, section N2.7.9	Proceeds of Crime Act, 2013; ⁹⁴⁴ Paragraph 11.12 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering.	Laundering and Proceeds of Crime Act, 2013	Laundering and Proceeds of Crime Act, 2013
-------------------	--	--	--

⁹⁴⁴ Act 4 of 2013.

9.7 Level of Compliance with Recommendation 20: STRs

All fourteen SADC countries AML/CFT Law and or Regulations contain a provision on suspicious transaction reporting and in all cases, suspicious transactions including attempted transactions must be reported to the FIU [FATF Recommendation 20]. Some jurisdictions provide specific guidance on when “attempted transactions” should be seen as suspicious. The Namibian Guidance Note No. 1 on Suspicious Transaction Reporting, 2009 makes it clear that not only completed suspicious transitions must be reported, but also ‘attempted transactions’.⁹⁴⁵ The Note however warns that an attempt to conduct a transaction does not necessarily mean the transaction is suspicious. However, the circumstances surrounding it might contribute to reasonable grounds for suspicion. Practical examples are given of what might constitute an ‘attempted’ suspicious transaction. Other countries in the region should be encouraged to issue similar practical advice to accountable institutions.

Examples of attempted transactions, as set out in the Namibian Guidance Note No. 1 on Suspicious Transaction Reporting, 2009 are set out in Table 73 below.

Table 73: Examples of Attempted Transactions

Example	Detail
Refusal to provide ID when attempting to make a deposit	A client approaches a financial institution or casino to make a deposit, but the financial institution or casino refuses to accept the deposit because the client refuses to provide identification as requested
Insistence on using cash when buying securities or life insurance	A client approaches a securities dealer or life insurance agent to conduct a transaction, such as buying securities or life insurance, but the securities dealer or life insurance agent refuses to process the transaction because the client insists on using cash
Offer to purchase property not realized once ID requested despite large cash deposit	A client of a real estate agent starts to make an offer on the purchase of a house with a large deposit, but will not finalize the offer once asked to provide identification
Requesting an accountant to facilitate large cash transactions	An individual asks an accountant to facilitate a financial transaction involving large amounts of cash, but the accountant declines to conduct the transaction
Refusal to provide ID to a money services business	A client requests a money services business (i.e. a bureau de change) to transfer a large amount of funds, but the money services business refuses because the client requesting the transfer refuses to provide identification

Source: Guidance Note No. 1 on Suspicious Transaction Reporting, 2009

A lack of coordination, conflicting legislation and conflicting messages with respect to the reporting of suspicious transactions has however been highlighted by a number of countries as an area of concern.

⁹⁴⁵ Paragraphs 4.2.1 and 4.2.2 Guidance Note No. 1 on Suspicious Transaction Reporting, 2009.

For example, while section 17 of the Botswana Financial Intelligence Agency Act, 2009⁹⁴⁶ requires a specified party to within such period as may be prescribed, report a suspicious transaction to the Agency, Regulation 14 of the Banking (Anti-Money Laundering) Regulations, 1995 requires banks to report to both the Central Bank and the Financial Intelligence Agency. The National Payment System Department of the Bank of Botswana confirmed that the Financial Intelligence Agency is the principal institution responsible for receiving STRs despite the fact that the section 21(4) of the Banking Act⁹⁴⁷ states that 'a bank shall notify the Central Bank of any transaction by any of its customers which it suspects to be money laundering'⁹⁴⁸ and section 16A(15) of the Proceeds of Serious Crime Act, 1990 (As Amended)⁹⁴⁹ states that 'where a designated body that is party to the transaction in respect of which there are reasonable grounds to suspect that the transaction brings or will bring the proceeds of serious crime into its possession, or that it may facilitate the transfer of the proceeds of serious crime, the designated body shall, within ten days of becoming party to such transaction, report the suspicion to the Directorate and to the Regulatory Authority.'⁹⁵⁰ It is imperative that section 21(4) of the Banking Act, 1995⁹⁵¹ and section 16A(15) of the Proceeds of Serious Crime Act, 1990 (As Amended)⁹⁵² be amended as soon as possible as these sections are in direct contradiction with section 4(1)(a) of the Financial Intelligence Agency Act, 2009.⁹⁵³ In practice, banks are submitting STRs to Financial Intelligence Agency and copies are still sent to Bank Supervision, as the FIA is not yet fully operational.⁹⁵⁴ The Directorate of Corruption and Economic Crime (DCEC) are however under the impression that they still have residual responsibility for receiving STRs and noted that a lack of coordination, conflicting legislation and conflicting messages with respect to the reporting of suspicious transactions is a key concern. An interview with the FIU however, revealed that the FIU are under the impression that the Bank of Botswana is the default "receiver" of STRs as the FIU does not have the operational capacity to receive STRs yet.

A similar problem is reportedly experienced in Lesotho. The Financial Intelligence Centre representatives confirmed that the Financial Intelligence Unit has not received any STRs from the commercial banks in Lesotho. These are allegedly being sent to the Central Bank but the interviewees were not sure to which department (Supervision or Excon) they are being sent. There is currently no reporting system in place. The Financial Intelligence Unit has procured the IMBl2 system (software) but this has not been implemented as yet. The Financial Intelligence Centre is however currently in consultation with the commercial banks to agree upon the reporting format and requirements.⁹⁵⁵ The deadline for the conclusion of consultations was set for the end of February 2013 with the planned implementation deadline being the end March.

Swaziland is an example of another country that appears to have conflicting provisions in its domestic legislation with respect to the reporting of suspicious transactions. The obligation for accountable institutions, the supervisory authority or an auditor of an accountable institution to report suspicious transactions are set

⁹⁴⁶ Act 6 of 2009.

⁹⁴⁷ Act 13 of 1995.

⁹⁴⁸ Section 21(4).

⁹⁴⁹ Act 19 of 1990 (As Amended).

⁹⁵⁰ Directorate of Corruption and Economic Crime (DCEC).

⁹⁵¹ Act 13 of 1995.

⁹⁵² Act 19 of 1990 (As Amended).

⁹⁵³ Act 6 of 2009.

⁹⁵⁴ Banks are reported to have Banks do have people that are monitoring low value transactions. If they see a trend they have been red flagging multiple transactions and reporting these as suspicious transaction.

⁹⁵⁵ The two individuals interviewed in February 2013 stated that "banks have not agreed upon whether reporting will be online or manual and there is a need to accommodate what banks want".

out in section 12 and section 13 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. Accountable institutions are required to report the suspicious transaction or attempted transaction to the Swaziland Financial Intelligence Unit (SFIU) no later than two days after forming the suspicion.⁹⁵⁶ The law specifically states that the report made shall be in writing and may be given by way of mail, telephone to be followed up in writing, fax or electronic mail or such other manner as may be prescribed by the SFIU.⁹⁵⁷ Several of the commercial banks interviewed during March 2013 expressed the concern that section 12 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 is in conflict with the wording in section 38 of the Financial Institutions Act, 2005.⁹⁵⁸ This section reads:

“38 (1) No financial institution shall carry out a transaction which it knows or suspects to be related to a serious criminal activity until it reports the information regarding the transaction that indicates such activity to the Bank.”

Several commercial banks in Swaziland seem to be unsure of whether they should process the transaction even if they suspect or have reasonable grounds to suspect that the transaction or attempted transaction may be related to the commission of an unlawful activity, a money laundering offence or an offence of financing of terrorism and then report the transaction to the SFIU as seems to be the intent behind s12 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 or not process the transaction at all, as seems to be the intent behind section 38(1) if the Financial Institutions Act, 2005. The Financial FATF, 2013 Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion report notes that with respect to the requirement to report suspicious transactions, “the risk-based approach is appropriate for the purposes of identifying potentially suspicious activity, for example by directing additional resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk. As part of an RBA, it is also likely that a financial institution will utilise information (typologies, alerts, guidance) provided by competent authorities to inform its approach for identifying suspicious activity (FATF, 2013).” An example of such a typology/guidance is provided by the South African FIC in paragraph 4.1 of Guidance Note 4 that sets out a number of indicators that can be used when evaluating transactions. The list is by no means exhaustive and is “intended merely to guide persons involved in businesses to identify those situations that should raise questions or give rise to the sense of discomfort, apprehension or mistrust (FIC, 2008).”

Examples, extracted from the indicators listed in paragraph 4.1 are reflected in Table 74 below.

Table 74: Indicators of Suspicious and Unusual Transactions

Category	Indicator
Unusual business	<ul style="list-style-type: none"> • Deposits funds with the request for immediate transfer elsewhere • Unwarranted and unexplained international transfers • Transactions do not appear to be in keeping with normal industry practices • A transaction seems to be unusually large or otherwise inconsistent with the customers financial standing or usual pattern of activities
Knowledge of Reporting or Record Keeping	<ul style="list-style-type: none"> • A customer attempts to convince employee not to complete any documentation required for the transaction • A customer makes enquiries that would indicate a desire to avoid reporting

⁹⁵⁶ Section 12(1)(b)(ii) Money Laundering and Financing of Terrorism (Prevention) Act, 2011.

⁹⁵⁷ Section 12(2)(a).

⁹⁵⁸ Act 6 of 2005.

Requirements	<ul style="list-style-type: none"> • A customer seems very conversant with money laundering and terrorist financing issues • A customer is quick to volunteer that funds are clean or not being laundered
Identification	<ul style="list-style-type: none"> • The use of seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar but different addresses and, in particular, the opening or operating of a false name account • Opening accounts using false or fictitious names • A customer changes a transaction after learning that he must provide a form of identity • A customer only submits copies of personal identification documents
General	<ul style="list-style-type: none"> • A customer provides insufficient vague or suspicious information concerning a transaction • Accounts that show unexpectedly large cash deposits and immediate withdrawals • A frequent exchange of small denomination notes for larger denomination notes • Involvement of significant amounts of cash in circumstances that are difficult to explain

Source: FIC Guidance Note 4

In Malawi, Regulation 27(1)(b) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 specifically requires the Compliance Officer to apply internal risk management procedures to suspicious transaction disclosures from officers and employees of the financial institution and only to report disclosures deemed to be suspicious to the FIU.

Paragraph 8.03 of the Mauritian Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005 also introduces the risk-based approach and lists several questions that financial institutions might consider when determining whether an established customer's transaction might be suspicious. These are:

- is the size of the transaction consistent with the normal activities of the customer?
- is the transaction rational in the context of the customer's business or personal activities?
- has the pattern of transactions conducted by the customer changed?
- where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Most SADC Member States do not however provide guidance on the application of the RBA for the purpose of identifying potentially suspicious activity, for example, by directing resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk.

The result of this is, that, "large, sophisticated institutions reported that they have comprehensive product ML/FT risk assessment processes. Smaller institutions sometimes have rudimentary processes and, more often, do not undertake risk-assessment measures at all. Guidance that would enable large institutions in the region to improve their processes and empower smaller institutions would be very helpful."⁹⁵⁹ The AFI/ESAAMLG report states further that, "many institutions that have classified products as low-risk products

⁹⁵⁹ Alliance for Financial Inclusion (AFI) and Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *Public and Private Sector Surveys Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices* 31.

and have filed suspicious transaction reports in respect of those products have been unable to provide any statistics on the number of such reports that were filed, compared to the number of reports files in terms of standard and higher-risk products. Monitoring of risks posed by products that were classified as low-risk is important to ensure that the internal classification was correct. Guidance on the appropriate monitoring and management of risks posed by low-risk products and clients will be helpful.

Table 75: Compliance with FATF Recommendation 20: Suspicious Transaction Reporting

Rec. 20 STR	STR Statutory Reference	AML/CFT Law and or Regulations contain a provision on suspicious transaction reporting	All suspicious transactions including attempted transactions must be reported, regardless of the amount	Law mandates that suspicious transaction reports must be submitted to the FIU	Conflicting provisions found in other laws and regulations	Guideline or guidance note on how suspicious transactions should be reported
Angola See Annexure A, section A2.7.10	Article 13(1) of Law n° 34/11	✓	✓	✓	✗	✗
Botswana See Annexure B, section B2.7.10	Part IV Financial Intelligence Agency Act, 2009 ⁹⁶⁰	✓	✓	✓	✓ S 21(4) Banking Act ⁹⁶¹ S16A(15) Proceeds of Serious Crime Act, 1990 (As Amended) ⁹⁶²	✗
DRC See Annexure C, section C2.7.10	Articles 20 to 23 and 28 of Law n° 04/016	✓	✓ ⁹⁶³	✓	✗	✗

⁹⁶⁰ Act 6 of 2009. Reporting obligation and cash transactions are the subject matter of Part IV section of the Financial Intelligence Agency Act 6 of 2009. This Part of the Act covers inter alia the obligation to report suspicious transactions (section 17), the reporting of cash transactions above prescribed limit (section 18) and general reporting (section 19). Section 17 of the Act reads “a specified party shall, within such period as may be prescribed, report a suspicious transaction to the Agency” and section 19(1) “a person who carries on, is in charge of, manages, or is employed by a business, shall report a suspicious transaction to the Agency.” No Guidelines or Guidance Notes have been issued by the FIA on how suspicious transactions should be reported. The application of a risk-based approach to this issue has not been documented or communicated to specified parties.

⁹⁶¹ Act 13 of 1995.

⁹⁶² Act 19 of 1990.

⁹⁶³ All transactions provided for must be reported before they are carried out.

Lesotho See Annexure D, section D2.7.10	S18 and S23 of the Money Laundering and Proceeds of Crime Act, 2008 ⁹⁶⁴	✓	✓ ⁹⁶⁵	✓	✗	✗
Malawi See Annexure E, section E2.7.10	S28(1) Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 ⁹⁶⁶	✓	✓	✓	✗	✗
Mauritius See Annexure F, section F2.7.10	S14 Financial Intelligence and Anti-Money Laundering Act, 2002 ⁹⁶⁷	✓	✓	✓	✗	✓ ⁹⁶⁸
Mozambique See Annexure G, section G2.7.10	Article 18(1) Law nº 14/2013	✓	✓	✓	✗	✗

⁹⁶⁴ Act 4 of 2008.

⁹⁶⁵ The law requires that such reports must be made within the prescribed period and wherever possible before the transaction is carried out.

⁹⁶⁶ Act 11 of 2006. This section covers two different types of reporting. Firstly, large cash transaction reporting and secondly, suspicious transaction reporting. In addition, section 29 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 provides that whenever a supervisory authority or auditor suspects or has reasonable grounds to believe that information it has related to any transaction or attempted transaction that may involve a money laundering offense, the financing of terrorism, or may be of assistance in the enforcement of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006⁹⁶⁶, shall report such transaction or attempted transaction to the FIU. The FIU confirmed in a meeting held with them in May 2013 that the STR reporting process in Malawi is currently a manual process although all transactions are sent to FIU electronically in an encrypted format. All reporting institutions are required to report to the FIU on a weekly basis.

⁹⁶⁷ Act 6 of 2002.

⁹⁶⁸ Paragraph 8 of the Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions, 2005; Guidance Note 2 (2009): Suspicious Transaction Report.

Namibia See Annexure H, section H2.7.10	Sections 33(1) and S33(2) Financial Intelligence Act 2012 ⁹⁶⁹	✓	✓	✓	✗	✓ ⁹⁷⁰
Seychelles See Annexure I, section I2.7.10	S10 Anti-Money Laundering Act, 2006 (As Amended) ⁹⁷¹	✓	✓	✓	✗	✓ ⁹⁷²
RSA See Annexure J, section J2.7.10	S29 of the Financial Intelligence Centre Act, 2001 (As Amended); ⁹⁷³ Regulations 22 to 24 Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended)	✓	✓	✓	✗	✓ ⁹⁷⁴
Swaziland See Annexure K, section	S12 and S19 of the Money Laundering and Financing of	✓	✓	✓	✓ S38 of the Financial Institutions Act,	✗

⁹⁶⁹ Act 13 of 2012.

⁹⁷⁰ Guidance Note No. 1 of 2009 on Suspicious Transaction Reporting; Guidance Note No. 4 of 2009 on the Implementation of a Compliance Regime.

⁹⁷¹ Act 5 of 2006.

⁹⁷² Paragraphs 16 to 19 of the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities, 2007.

⁹⁷³ Act 38 of 2001 (As Amended).

⁹⁷⁴ Guidance Note 4 on Suspicious Transaction Reporting. This Guidance Note was issued by the Financial Intelligence Centre in March 2008.

K2.7.10	Terrorism (Prevention) Act 2011				2005 ⁹⁷⁵	
Tanzania See Annexure L, section L2.7.10	S6(a) of the Anti-Money Laundering Act, 2006 (As Amended); ⁹⁷⁶ Regulations 22 to 27 Anti-Money Laundering Regulations, 2012	✓	✓	✓	✗	✗
Zambia See Annexure M, section M2.7.10	S29 Financial Intelligence Centre Act, 2010; ⁹⁷⁷ Directive 11 Anti-money Laundering Directives, 2004	✓	✓	✓	✗	✗
Zimbabwe See Annexure N, section N2.7.10	S30 Money Laundering and Proceeds of Crime Act, 2013; ⁹⁷⁸ Section 26 of the Bank Use Promotion and Suppression of Money Laundering	✓	✓	✓	✗	✓ ⁹⁸⁰

⁹⁷⁵ Act 6 of 2005.

⁹⁷⁶ Act 12 of 2006 (As Amended).

⁹⁷⁷ Act 46 of 2010.

⁹⁷⁸ Act 4 of 2013.

	Act, 2004 (As Amended) ⁹⁷⁹					
--	---------------------------------------	--	--	--	--	--

⁹⁸⁰ Paragraphs 14 and 15 of Guideline No. 01-2006 BUP/SML: Anti-Money Laundering provides guidance on the recognition of a suspicious transaction and reporting of suspicious transactions respectively. Appendix E provides examples of suspicious transactions. With respect to the format in which suspicious transactions must be submitted to the Unit, the Unit informed us that they currently use a pro-forma form that is emailed by accountable institutions. The Unit apparently did have automated software, but this has not been running.

⁹⁷⁹ [Chapter 24:24].

9.8 Level of Compliance with Recommendation 34: Guidance and Feedback

The Financial Intelligence Unit in all fourteen SADC countries is empowered to issue guidelines and guidance notes. However, the wording of these sections in either the AML Law or its supporting regulations differs from country. Some drafters have used the words 'may issue guidelines', which upon the normal interpretation of these words infers that the issuing of guidelines is at the discretion of the Financial Intelligence Unit while others have used the words 'shall issue guidelines.' Guidelines and or guidance notes have not been issued by the Financial Intelligence Unit, the Central Bank, or other Supervisory Authorities, in six SADC countries.

The levels of feedback from the Financial Intelligence Unit to accountable institutions, particularly with respect to feedback on suspicious transaction reports received, vary extensively from country to country.

In Malawi for example, it is noted in the 2012 ESAAMLG Mutual Evaluation that, "the FIU has not provided any feedback to reporting institutions, other than acknowledgement of the receipt of reports. This is still a very new process for banks in Malawi. Others have not begun to make suspicious transaction reports. Some banks have received acknowledgements of their submissions, while others have not received any acknowledgments."⁹⁸¹ In South Africa, on the other hand, "the Centre provides general feedback, acknowledging receipt of all reports and providing the reporter with a unique reference number which will be used in respect of further communication relating to a particular report. As a general rule, the Centre does not provide case-by-case feedback on the outcomes of analysis and referral processes relating to information reported to it, as this may prompt an institution to change its behaviour towards a customer which may, in turn, alert the customer to the fact that a report has been made in respect of a transaction, or may generate unwarranted suspicious and unusual transaction reports. Nevertheless, in specific instances the Centre may engage with a reporting person/entity subsequent to receiving a report, in order to obtain additional information or to ascertain whether a transaction should be stopped by means of the Centre's intervention powers."⁹⁸²

Table 76: Compliance with FATF Recommendation 34 Guidance and Feedback

Rec. 34 Guidance & Feedback	Statutory Reference	FIU/FIA/FIC mandated by law or regulation to issue guidelines or guidance notes	FIU/FIA/FIC or Central Bank have issued Guidelines and or Guidance Notes
Angola See Annexure A, section A2.7.11	Article 39 (Information Dissemination) and Article 40 (Information Feedback) Law n° 34/11	✓	✗

⁹⁸¹ Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the World Bank 2008 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: The Republic of Malawi*.

⁹⁸² Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2009 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: South Africa*.

Botswana See Annexure B, section B2.7.11	S4 Financial Intelligence Agency Act, 2009 ⁹⁸³	✓ ⁹⁸⁴	✗
DRC See Annexure C, section C2.7.11	Article 17 of Law n° 04/016	✓ ⁹⁸⁵	✗
Lesotho See Annexure D, section D2.7.11	S15(2)(e) Money Laundering and Proceeds of Crime Act, 2008 ⁹⁸⁶	✓	✓ ⁹⁸⁷
Malawi See Annexure E, section E2.7.11	Regulation 29(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011	✓	✗
Mauritius See Annexure F, section F2.7.11	Regulation 18(1)(a) Financial Intelligence and Anti-Money Laundering Regulations 2003 (As Amended)	✓	✓
Mozambique	Article 21 and Article 22 Law n° 14/2013	✓ ⁹⁸⁸	✗

⁹⁸³ Act 6 of 2009.

⁹⁸⁴ Section 4 of the Financial Intelligence Agency Act, 2009⁹⁸⁴ sets out the functions of the FIA and specifically mandates the FIU to give guidance to a specified party regarding the performance by the specified party of duties under the Act and provide feedback to a specified party regarding a report made in accordance with the Act. As the FIA is not fully operational, the Agency has not provided any guidance or feedback to specified parties yet.

⁹⁸⁵ Article 17 of Law n° 04/016 mandates the Financial Intelligence to collect and process financial information relating to money-laundering channels and terrorism financing. With respect to its role in providing guidance and feedback, the Financial Intelligence Unit is required to inter alia: carry out periodic assessments on the development of money-laundering and terrorism financing techniques used in the country and issue opinions on the State's anti-money-laundering and terrorism financing policy and the implementation thereof. The FIU is also required to propose such reforms as may be necessary to make anti-money-laundering efforts more effective. Quarterly progress reports and an annual summary report must be prepared by the FIU and be submitted to the Ministry of Finance and copied to the Ministry of Justice and the Governor of the Central Bank of Congo.

⁹⁸⁶ Act 4 of 2008.

⁹⁸⁷ To date, the guidelines that have been issued have been issued by the Central Bank of Lesotho and not the FIU. The Unit is not fully operational.

⁹⁸⁸ Article 21 of Law n° 14/2013 states that, "it is the responsibility of the supervisory authorities as well as of the FIFiM, within the scope of their assignments and legal competencies to issue warnings and disseminate up-to date information regarding the tendencies and practices known, with the objective of preventing money laundering and funding of terrorist activities." Law n° 14/2013 contains a specific article on feedback. Article 22 reads, "the GIFiM must provide opportune feedback on information provided to the financial authorities, non- financial bodies and supervisory authorities relating to

See Annexure G, section G2.7.11			
Namibia See Annexure H, section H2.7.11	S9(1)(h) Financial Intelligence Act 2012 ⁹⁸⁹	✓ ⁹⁹⁰	✓ ⁹⁹¹
Seychelles See Annexure I, section I2.7.11	Table in the Anti-Money Laundering Amendment Act, 2008 ⁹⁹²	✓	✓ ⁹⁹³
RSA See Annexure J, section J2.7.11	S4(c) Financial Intelligence Centre Act, 2001 (As Amended); ⁹⁹⁴ Regulation 28(1) Money Laundering and Terrorist Financing Control Regulations, 2002 (As Amended)	✓	✓ ⁹⁹⁵
Swaziland	S12(4) Money Laundering and Financing of	✓ ⁹⁹⁶	✓ ⁹⁹⁷

the progress and results on the communication of suspicious transactions relating to money laundering and funding of terrorist activities.”

⁹⁸⁹ Act 13 of 2012.

⁹⁹⁰ . Part 2 of the Financial Intelligence Act 13 of 2012 contains the provisions applicable to the Financial Intelligence Centre, its administration and staff. As per section 9(1)(h), one of the functions of the Centre is to, “give guidance to Accountable and reporting institutions to combat money laundering or financing of terrorism activities.” The Centre is further empowered to, “issue determinations to any supervisory body in terms of which the supervisory body must enforce compliance by an accountable or reporting institution regulated by such supervisory body.”

⁹⁹¹ All of the Guidance Notes issued to date have been were issued by the FIC BON pursuant to section 5(2) and 5(3) of the now repealed Financial Intelligence Act, 2007.

⁹⁹² Act 18 of 2008.

⁹⁹³ Only one Guideline has been issued by the FOI to date.

⁹⁹⁴ Act 38 of 2001 (As Amended).

⁹⁹⁵ The Financial Intelligence Centre FIC is by far the most proactive financial intelligence centre in the SADC region with respect to issuing guidance notes and PCCs. To date, the Financial Intelligence Centre (FIC) has issued six guidance notes and twenty one PCC covering a number of important topics.

⁹⁹⁶ Section 12(4) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 MLFPA is the only section in the Act that requires the SFIU to give feedback to accountable institutions. This feedback is only in the case where the SFIU has reasonable grounds to suspect that a transaction or a proposed transaction may involve an offence of financing of terrorism, the proceeds of an unlawful activity or a money laundering offence. Under these circumstances, the SFIU may direct the accountable institution in writing or by telephone to be followed up in writing within 1 working day, not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period as may be determined by the SFIU, which may not be more than five working days, in order to allow the SFIU to make necessary inquiries concerning the transaction; and if the SFIU deems it appropriate, to inform and advise a competent authority. The Act does not require the SFIU to provide feedback to accountable institutions under any other circumstances although section 31 (h) requires the SFIU to compile

See Annexure K, section K2.7.11	Terrorism (Prevention) Act 2011		
Tanzania See Annexure L, section L2.7.11	Section 6 Anti-Money Laundering Act, 2006 (As Amended), ⁹⁹⁸ Regulations 34 and 34 Anti-Money Laundering Regulations, 2012	✓	✓
Zambia See Annexure M, section M2.7.11	S56 Financial Intelligence Centre Act, 2010 ⁹⁹⁹	✓	✓
Zimbabwe See Annexure N, section N2.7.11	S4(e) Bank Use Promotion and Suppression of Money Laundering Act, 2004 (As Amended) ¹⁰⁰⁰	✓	✓

Several of the private sector stakeholders interviewed during the course of the research noted the lack of feedback and guidance from the Financial Intelligence Unit in their country as an area of frustration and concern. In this regard, the *Public and Private Sector Survey Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices* report that succinctly presents the results of a private sector survey of money laundering (ML) and terrorist financing (TF) risk assessment and risk mitigation practices relating to the low-income sector notes that the private sector requested engagement and guidance to ensure compliance and greater consistency in a number of areas. These include: simplified due diligence measures, measures to assist specific vulnerable groups, identification of Politically Exposed Persons (PEPs) and persons subject to United Nations Security Council (UNSC) sanctions, product and client- risk assessments, monitoring of risk levels, combating identity fraud in relation to low- risk products, integrity measures in relation to employees and agents, and guidance and training on identification of fake documentation.

statistics and records and disseminate information within Swaziland or elsewhere, as well as to make recommendations arising out of any information received and section 31(k) for the SFIU to provide training.

⁹⁹⁷In Swaziland, it appears that the Supervisory Authorities are responsible for issuing guidelines to accountable institutions under their supervision. This reasoning is derived from the fact that section 31(i) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 states that “the SFIU is required to issue guidelines to accountable institutions **not under the jurisdiction of supervisory authorities** in relation to customer identification, record keeping and, reporting obligations and the identification of suspicious transactions.

⁹⁹⁸ Act 12 of 2006 (As Amended).

⁹⁹⁹ Act 46 of 2010.

¹⁰⁰⁰ [Chapter 24:24].

SECTION 10: RECOMMENDATIONS

10.1 SADC Wide Findings and Recommendations

This project has revealed substantial differences in the regulatory models adopted, the level of sophistication of the legal and regulatory framework, differences in legal traditions (civil law v common law), available infrastructure (RTGS, ACH and National Switches), organisational capacity and the overall approach to the regulation and oversight of the National Payment System, in each country. While countries such as Namibia and South Africa have advanced legal frameworks, others such as Lesotho, Malawi, Mauritius and the DRC do not have a National Payment System Act in place. As such, vital provisions that are applicable to the regulation and oversight of their domestic National Payment System, such as settlement finality and irrevocability, access criteria, transfer orders and netting, the insulation of collateral security from the effects of insolvency law and general override provisions in the case of curatorship, judicial management or liquidation do not exist in a legally enforceable Act.

For countries that do have a legally enforceable National Payment System Act or Payment System Management Act in place, several gaps and inconsistencies across the legal and regulatory frameworks have been identified. When compared against the international best practice hard law benchmark used for the purposes of undertaking a benchmarking exercise, namely the EU Regulations and Directives, it is apparent that none of the National Payment System Acts applicable domestically contain any provisions pertaining to cross-border relations and transactions.¹⁰⁰¹

In light of the introduction of SIRESS, it is vital that domestic laws are harmonised, that regulators are legally mandated to cooperate with each other and that provisions pertaining to cross-border payment arrangements are included in domestic laws. A particular area of concern is the choice of an appropriate regional dispute resolution mechanism and fora. While several National Payment System Acts contain provisions for the choice of conciliation, mediation and arbitration as the means to resolve disputes between participants in domestically designated systems, none of the Acts contain provisions on international arbitration, the choice of law or appropriate fora. It is also specifically noted that none of the National Payment System Acts contain dispute settlement provisions applicable to payment service providers and payment service users. This matter is covered in Regulation (EC) No 924/2009 on Cross-Border Payments in the Community, and, in light of the

¹⁰⁰¹ An example of such a provision is found in *Directive 98/26/EC*. Articles 6 and 10 of Directive 98/26/EC as amended by Directive 2009/44/EC require Member States to notify to the Commission of which systems they have designated and which national authorities are in charge of notification. The Commission holds two registers with this information. They are up-dated whenever Member States send new information to the Commission. Specifically, Article 10(1) reads: "Member States shall specify the systems, and the respective system operators, which are to be included in the scope of this Directive and shall notify them to the Commission and inform the Commission of the authorities they have chosen in accordance with Article 6(2). The system operator shall indicate to the Member State whose law is applicable the participants in the system, including any possible indirect participants, as well as any change in them. In addition to the indication provided for in the second subparagraph, Member States may impose supervision or authorisation requirements on systems which fall under their jurisdiction. An institution shall, on request, inform anyone with a legitimate interest of the systems in which it participates and provide information about the main rules governing the functioning of those systems."

introduction of SIRESS and the possible addition of various retail streams in the future, this should be considered by SADC Member States.¹⁰⁰²

Most countries do not have a well-structured legal and regulatory framework for retail payments. Vital issues such as electronic money (E-Money), card payments, agent banking, the authorisation of payment service providers, the issuance of payment instruments and the rights and obligations of PSPs and users are generally poorly covered, if at all. The lack of law and regulation in the SADC region covering these matters is highlighted as an additional area of concern.

While individual SADC Member States are at liberty to amend their domestic laws and regulations as they see fit, we recommend that this is carried out in a coordinated manner through the drafting of a model law(s). Several SADC Protocols including the Protocol of Finance and Investment require State Parties to create Model Laws for the Region. Article 2 of Annex 5 of the Protocol on Finance and Investment requires State Parties to “promote the mutual co-operation, co-ordination and harmonisation of the legal and operational frameworks of Central Banks which shall culminate in the creation of a Model Central Bank Statute for the Region as contemplated by the RISDP.”

It must be noted that Model Laws are by their very nature, “soft laws” and are not legally enforceable. They are however generally used to guide governments in the crafting and amendment of their own domestic laws. Model Laws are primarily aimed at assisting member states, in particular policy makers and legislative drafters to address all the relevant areas in need of legislative reform without usurping the authority of national legislatures. In an article entitled “Judges Welcome SADC Model Law on HIV/AIDS” the author notes that, “an important benefit of the Model law is that it builds on the collective experiences of other legislatures, providing a pool of wisdom from which a particular legislature may select and adapt provisions to suit its own circumstances and needs.”¹⁰⁰³ Given the current organisational and institutional limitations of the SADC it is submitted that the appropriate instruments to be drafted to spearhead the harmonisation process at this time, are model laws that could be used by each SADC Member State as best practice benchmarks.¹⁰⁰⁴

The recommendations below are high priority short-term action areas.

Recommendation 1: Glossary of Key Terms

¹⁰⁰² According to Article 11 of the Regulation (EC) No 924/2009, Member States are required to establish adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and their payment service providers. Member States were required to notify the Commission of their out-of-court complaints and redress bodies by 29 April 2010.

¹⁰⁰³ Magadza M 2009 *Judges Welcome SADC Model Law on HIV/AIDS*. Online. Available at: <http://www.africafiles.org/article.asp?ID=22152>

¹⁰⁰⁴ See Bilal 2005 *Can the EU Be a Model of Regional Integration? Risks and Challenges for Developing Countries* where the author notes that, “Some aspects of the EU model, which is a complex mix of intergovernmental and supranational approaches, have not been carried over to some other regional groupings. Most developed countries, while calling for greater integration, have also resisted the delegation of sovereignty that would have been necessary to development effective supranational institutions, preferring to rely more heavily on an intergovernmental model of integration (Mattli, 2003). This resistance has also contributed to put the institutional design and policy agenda of some of the regional groupings (e.g. ECOWAS, SADC, Mercosur, etc.) at odds with the effective implementation of their integration programmes.”

Section 2.3.2 of each country report highlights substantial gaps in each country's defined terms. Where terms are defined, significant differences in the definitions used have also been identified. It is highly recommended that a glossary of key terms is prepared.

Recommendation 2: Model Laws (National Payment System and Payment Services)

At present, a harmonised legal and regulatory framework for payments does not exist in SADC and the region also faces a number of organisational and institutional challenges. The SADC Central Bank¹⁰⁰⁵ is yet to be established and SADC does not have a Parliament with legislative powers as in other similar institutions such as the EAC, EU and ECOWAS. There are no SADC Regulations and or Directives on Payments (Annex 6 of the Finance and Investment Protocol however establishes a framework for cooperation and coordination between Central Banks on payment, clearing and settlement systems)¹⁰⁰⁶ and the SADC Tribunal remains disbanded. As a result, the SADC Member States participating in the SIRESS proof of concept project have elected to structure the legal arrangements between participants through a number of multilateral agreements.¹⁰⁰⁷ These agreements have been drafted as a short term solution in order to provide for legal certainty until such time as an appropriate SADC wide legal and regulatory framework has been developed and adopted. Over the longer term, all fourteen SADC countries are committed to harmonising their legal and regulatory frameworks and to establishing the institutional and organisational structures conducive to the establishment of an integrated payments market.

As a key starting point in the harmonisation process, it is recommended that two SADC payments related model laws be drafted for discussion. These would be a Payment Systems Law to harmonise the provisions found in the current National Payment System Law in each SADC country and a Payment Services Law to introduce a harmonised legal framework for payment services thereby ensuring that cross-border payments within the SADC (particularly credit transfers, direct debits and card payments) can be carried out just as easily, efficiently and securely as domestic payments within the various Member States. These two Model Laws should be drafted taking into consideration international best practice principles, best practice provision drawn from the domestic law of SADC Member States and making use of the various EU Regulations and Directives as they pertain to specific cross-border matters.

Recommendation 3: Model Law (AML/CFT)

In theory, Article 9(3) of Annex 12 of the FIP establishes the SADC Anti-Money Laundering Committee. In practice however, this Committee has not been constituted and is therefore not, at this point in time, an official SADC structure. It is therefore recommended that the findings and recommendations as they relate to the

¹⁰⁰⁵ See *Clearit: The Swiss Professional Journal for Payment Traffic Edition 47 | March 2011* where it is noted that, "the SADC Central Bank is scheduled to be founded no later than 2018, in order to subsequently introduce the new single currency. However, the hurdles on the way to a successful economic integration of the SADC region are comparable to those in the first African example. The single market (2015) and the monetary union (2016) need to become a reality first. How can such projects be realised in such a short period in Africa, when it took Europe decades to do the same? Especially considering that many of these projects – such as linking the stock exchanges – lack the necessary funds?"

¹⁰⁰⁶ The SADC Summit has power to legislate pursuant to Article 10.3 of the SADC Treaty which clearly states that 'the Summit shall adopt legal instruments for the implementation of the provisions of this Treaty; provided that the Summit may delegate this authority to the Council or any other institution of SADC as the Summit may deem appropriate'.

¹⁰⁰⁷ There are currently three agreements and an MOU in place. These are the SIRESS Stakeholders Agreement, SIRESS Settlement Agreement, SIRESS Service Agreement and Schedules and the MOU for SADC Payment System Oversight.

harmonisation of specific provisions in AML laws and regulations as contained in this report and fourteen country annexures be considered in the short term by an existing SADC structure which has appropriate decision making powers in order to avoid the risk of in-action or substantially delayed action while the SADC Anti-Money Laundering Committee is being constituted.

In order to move towards the defined level of harmonisation of AML/CFT laws and regulations and not to be delayed by institutional matters, it is recommended that each SADC country be encouraged and guided by a duly mandated existing SADC structure, potentially the CCBG Legal-Sub Committee or the SADC Payment Steering Committee as duly mandated by the CCBG, to obtain a defined level of legislation and regulation at a national level in line with the revised FATF Recommendations (2012). It is recommended that the focus of mandated existing SADC structure should be directed towards:

- A: the drafting of an appropriate SADC Model AML/CFT Law and support being provided to domestic regulatory authorities during the process of amending domestic AML/CFT laws and regulations (see Recommendation 2 below);
- B. the commissioning and undertaking of a supra-national SADC wide risk assessment;
- C: the preparation of a short term action plan and a longer term hand-over plan. It is recommended that the mandated SADC structure works collaboratively with the ESAAMLG so as to avoid the duplication of efforts and resources.

Over the longer term, it is essential that the Anti-Money Laundering Committee as established by Annex 12 of the FIP is actually constituted, that a chair is appointed and the Committee be formally tasked with carrying the harmonisation work forward. This committee, once constituted will have a vital role to play in ensuring that SADC Member States make appropriate amendment to their domestic laws and regulations, to define the strategic direction to achieve the objectives of Annex 12 and to initiate further research and other projects that will support State Parties in fulfilling these objectives.

Recommendation 4: Scoping Study and Preparation of an Electronic Money Guideline for SADC

The review of the statutory instruments regulating E-Money in Namibia and the DRC, as compared to the E-Money guidelines issued by various central banks has highlighted significant differences in *inter alia*: the understanding and definition of E-Money; whether E-Money constitutes deposit taking or not; conditions for authorisation; initial capital, own funds and safeguarding requirements. It is recommended that in an effort to assist Central Banks in the SADC to adopt a consolidated approach to E-Money that an in-depth study on E-Money is undertaken which should culminate in the drafting of an E-Money guideline for the SADC region.¹⁰⁰⁸ This work should be undertaken at the same time as the drafting of the Model Laws as these matters are not mutually exclusive and cross references to specific provisions should be made in the Model Laws and the E-Money Guideline.

10.2 Country Specific Recommendations

¹⁰⁰⁸ Activities include, determining a common definition and understanding of E-Money, regulatory principles, and policy and drafting a SADC specific regulatory framework in the form of a guideline.

Country specific recommendations are set out in the fourteen country reports (Annexure A to Annexure N) that form an integral part of this report. These country specific recommendations are framed within the context of the primary overall recommendation for SADC that a Payment System Model Law is developed. As such, there is convergence in several of the recommendations made. The proposed Model Laws will draw upon international best practice together with regional best practice benchmarks as discussed throughout this report.

There are a number of vital issues that need to be addressed by each Central Bank and other relevant regulatory authorities within each domestic context. While each SADC Member State is at liberty to pass new laws and or make changes to existing legislation of its own accord, it is strongly recommended that amendments to the National Payment System / Payment System Management Act / Clearing and Settlement System Acts and the Anti-Money Laundering Acts are made in accordance with the provisions contained in the proposed SADC Model Laws. The country specific finding and recommendations set out in the Annexures can be found in Volumes I and II of the Individual Country Reports that form and integral part of this report.

Volume	Country	Country Report Page References
VOLUME I		
Volume I	Angola	Page 1 - 58
Volume I	Botswana	Page 59 - 115
Volume I	DRC	Page 116 - 178
Volume I	Lesotho	Page 179 - 246
Volume I	Malawi	Page 247 - 313
Volume I	Mauritius	Page 314 - 381
Volume I	Mozambique	Page 382 - 443
VOLUME II		
Volume II	Namibia	Page 1 - 85
Volume II	Seychelles	Page 84 - 149
Volume II	South Africa	Page 150 - 244
Volume II	Swaziland	Page 245 - 305
Volume II	Tanzania	Page 305 - 380
Volume II	Zambia	Page 381 - 440
Volume II	Zimbabwe	Page 441 - 500

ANNEXURE O: TRANSPOSITION OF THE SETTLEMENT FINALITY DIRECTIVE INTO DOMESTIC REGULATION

The Irish Statutory Instrument S.I. No. 539/1998 - European Communities (Finality of Settlement in Payment and Securities Settlement Systems) Regulations, 1998 transposes the mandatory provisions of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems into domestic Irish law.¹⁰⁰⁹

Table O1: Content of Irish S.I. No. 539/1998

Regulation 2(1)	The following are defines: Bank; ¹⁰¹⁰ collateral security; ¹⁰¹¹ credit institution; ¹⁰¹² financial institution; ¹⁰¹³ member; ¹⁰¹⁴ the opening of insolvency proceedings; ¹⁰¹⁵ netting; ¹⁰¹⁶ payment system; ¹⁰¹⁷ payment system settlement agent; ¹⁰¹⁸ and transfer order. ¹⁰¹⁹
------------------------	---

¹⁰⁰⁹ The primary aim of the Directive to reduce the legal risks associated with participation in settlement systems, in particular as regards the legality of netting agreements and the enforceability of collateral security. The Directive's provisions apply to any EC payment or securities settlements system operating in any currency or the euro, any EC institution which participates in such a system, collateral security provided in connection with participation in such a system, and collateral security provided in connection with monetary policy operations.

¹⁰¹⁰ Bank means the Central Bank of Ireland.

¹⁰¹¹ means all realisable assets provided under a pledge (including money provided under a pledge), a repurchase or similar agreement, or otherwise, for the purpose of securing rights and obligations potentially arising in connection with a payment system or provided to central banks of the Member States of the European Union or to the European Central Bank.

¹⁰¹² Has the meaning assigned to it by the European Communities (Licensing and Supervision of Credit Institutions) Regulations, 1992 (S.I. No. 395 of 1992). In this Irish Statute, credit institution is defined as, "an undertaking, other than a credit union or friendly society, whose business it is to receive deposits or other repayable funds from the public and to grant credit on its own account".

¹⁰¹³ Means an undertaking other than a credit institution providing any one or more of the financial services set out in the Schedule to the European Communities (Licensing and Supervision of Credit Institutions) Regulations, 1992, (S.I. No. 395 of 1992).

¹⁰¹⁴ Means a credit institution or financial institution, a central counterparty, a settlement agent or a clearing house which is a member of a payment system and nothing in these Regulations shall prevent a member acting as a central counterparty, a settlement agent or a clearing house or carrying out part or all of these tasks.

¹⁰¹⁵ Means the granting by the High Court of an order for the winding-up of a member of a payment system.

¹⁰¹⁶ Means the conversion into one net claim or one net obligation of claims and obligations resulting from transfer orders within a payment system that a member or members either issue to, or receive from, one or more other members of the payment system with the result that only a net claim can be demanded or a net obligation be owed.

¹⁰¹⁷ Has the meaning set out in section 5 of the Central Bank Act 8 of 1997. In the Irish Central Bank Act, payment system is defined as, "a system established in the State, or proposed to be established in the State, by any person, in which credit institutions or financial institutions participate and which provides for— (a) all or any of the following, namely, the processing, handling, clearance and settlement of any means of payment or of any securities, or (b) the payment of any moneys by that means of payment, by or as between the members of the system or third parties, whether or not the processing, handling, clearance, settlement or payment of any of the moneys takes place in part or in whole within the State or outside the State."

¹⁰¹⁸ Means an entity providing to institutions or to a central counterparty participating in a payment system settlement accounts through which transfer orders within such systems are settled and, as the case may be, extending credit to those institutions and central counterparties for settlement purposes.

Regulation 2(2)	A word or expression that is used in these Regulations and is also used in Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998*, shall, unless the contrary intention is expressed, have in these Regulations the same meaning that it has in that Directive.
Regulation 3(1)	A transfer order within a payment system shall be binding, even in the event of insolvency proceedings against a member, and shall be binding on third parties, where the transfer order was entered into the payment system before the moment of opening of insolvency proceedings against the member.
Regulation 3(2)	Netting within a payment system shall be binding on members, even in the event of insolvency proceedings against a member, and shall be binding on third parties, where the transfer orders involved in the netting were entered into the payment system before the moment of opening of insolvency proceedings against the member.
Regulation 3(3)	Where a transfer order is entered into a payment system after the moment of opening of insolvency proceedings against a member of the payment system and the order is executed on the day of opening of insolvency proceedings against the member, the order shall be legally binding only if, after the order is executed, the settlement agent, the central counterparty or the clearing house can prove that they were not aware, and should not have been aware, of the opening of insolvency proceedings against the member.
Regulation 4	No law, regulation, rule or practice on the setting aside of contracts and transactions concluded before the moment of the opening of insolvency proceedings against a member of a payment system shall lead to the unwinding of a netting.
Regulation 4(1)	The rules of a payment system shall specify the moment at which a transfer order shall be considered to have been entered into the payment system.
Regulation 4(2)	A transfer order may not be revoked from the moment specified in accordance with paragraph (1) of this Regulation
Regulation 5(1)	The High Court shall notify the Bank immediately upon granting an order for the winding up of a member of a payment system.
Regulation 5(2)	Upon receipt of such notification, the Bank shall immediately notify the appropriate authorities in the other Member States of the European Union of the order.
Regulation 5(3)	In the event of the opening of insolvency proceedings against a member of a payment system, the rights and obligations of the member of the payment system arising from membership of the payment system prior to the opening of insolvency proceedings against the member shall not be affected in any way by the opening of insolvency proceedings against the member.
Regulation 6	Notwithstanding any provision to the contrary contained in the law of the State relating to bankruptcy, receivership, examinership or liquidation, where insolvency proceedings are commenced under the law of the State against a member of a payment system, the rights and obligations of the member arising from the participation of that member in the payment system shall be determined in accordance with the law of the Member State under which the payment system operates.
Regulation 7(1)	The rights of - (a) a member of a payment system to collateral security provided to it in connection with its

¹⁰¹⁹ Means -(a) any instruction by a member to place at the disposal of another member an amount of money by means of a book entry on the accounts of a credit institution, a central bank or a settlement agent, or any instruction which results in the assumption or discharge of a payment obligation as defined by the rules of the system, or (b) an instruction by a member to transfer the title to, or interest in, a security or securities by means of a book entry on a register, or otherwise.

	<p>participation in the payment system, and</p> <p>(b) central banks of the Member States and of the European Central Bank to collateral security provided to them, shall not be affected by insolvency proceedings against the member or against a counterparty to a central bank of a Member State or the European Central Bank which provided the collateral security and such collateral security may be realised for the satisfaction of those rights</p>
Regulation 7(2)	Where securities (including rights in securities) are provided as collateral security to members or to central banks of the Member States or to the European Central Bank, and their right (or that of any nominee, agent or third party acting on their behalf) with respect to the securities is legally recorded on a register, account or centralised deposit system located in a Member State of the European Union, the determination of the rights of such entities as holders of the collateral security in relation to those securities shall be governed by the law of that Member State.
Regulation 8	The operators of a payment system shall notify the Bank of the membership of the system, including any possible indirect participants, and shall immediately notify it of any change in the membership of the payment system.
Regulation 9	A holder of a licence issued under section 9 of the Central Bank Act, 1971 (No. 24 of 1971), shall inform any person with a legitimate interest of the payment systems of which it is a member and shall provide information about the main rules governing the functioning of those payment systems.

ANNEXURE P: TRANSPOSITION OF THE ELECTRONIC SIGNATURES DIRECTIVE INTO DOMESTIC REGULATION

Section 7 of the UK Electronic Communication Act, 2000 and the United Kingdom Electronic Signatures Regulation 2002 transpose the Electronic Signatures Directive into domestic law and regulation. Provisions relating to the admissibility of electronic signatures as evidence in legal proceedings were implemented by s7 of the Electronic Communications Act 2000. These provisions are set out in Table P1 below.

Table P1: Section 7 of the Electronic Communications Act 2000

Ref.	Subject	Provision
S7(1)	Admissibility of electronic signatures in legal proceedings	In any legal proceedings— (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and (b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.
S7(2)	Definition of electronic signature	For the purposes of this section an electronic signature is so much of anything in electronic form as— (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and (b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.
S7(3)	Certification of electronic signature	For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that— (a) he signature, (b) means of producing, communicating or verifying the signature, or (c) a procedure applied to the signature, is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

The United Kingdom *Electronic Signatures Regulations 2002* implement Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures into UK law. The implemented provisions of this Directive relate to the supervision of certification-service-providers, their liability in certain circumstances and data protection requirements for them. The Directive does not favour any specific technology. Replacing manual, paper-based processing with automated, electronic signing processes has enabled organisations large and small to significantly reduce the cycle times, errors and costs associated with getting customers, partners, supplier and employees to review and sign documents needed to close new business, authorise decisions, and move operations forward. The impact electronic signatures have on an organisation's ability to deliver superior customer service, increase operational efficiency and improve bottom line results has often far exceeded initial expectations.

Table P2: Content of United Kingdom Electronic Signatures Regulation 2002

Regulation 2	Definitions are provided for: advanced electronic signature; ¹⁰²⁰ certificate; ¹⁰²¹ certification-service-provider; ¹⁰²² electronic signature; ¹⁰²³ qualified certificate; ¹⁰²⁴ signatory; ¹⁰²⁵ signature-creation data; ¹⁰²⁶ signature-creation device; ¹⁰²⁷ signature-verification data; ¹⁰²⁸ signature-verification device; ¹⁰²⁹ voluntary accreditation; ¹⁰³⁰
Regulation 3(1)	It shall be the duty of the Secretary of State to keep under review the carrying on of activities of certification-service-providers who are established in the United Kingdom and who issue qualified certificates to the public and the persons by whom they are carried on with a view to her becoming aware of the identity of those persons and the circumstances relating to the carrying on of those activities.
Regulation 3(2)	It shall also be the duty of the Secretary of State to establish and maintain a register of certification-service-providers who are established in the United Kingdom and who issue qualified certificates to the public.
Regulation 3(3)	The Secretary of State shall record in the register the names and addresses of those certification-service-providers of whom she is aware who are established in the United Kingdom and who issue qualified certificates to the public.
Regulation 3(4)	The Secretary of State shall publish the register in such manner as she considers appropriate.
Regulation 3(5)	The Secretary of State shall have regard to evidence becoming available to her with respect to any course of conduct of a certification-service-provider who is established in the

¹⁰²⁰ Advanced electronic signature means, "means an electronic signature (a) which is uniquely linked to the signatory, (b) which is capable of identifying the signatory, (c) which is created using means that the signatory can maintain under his sole control, and (d) which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

¹⁰²¹ Certificate means, "An electronic attestation which links signature-verification data to a person and confirms the identity of that person."

¹⁰²² Certification service-provider means, "A person who issues certificates or provides other services related to electronic signatures.

¹⁰²³ Electronic signature means, "Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

¹⁰²⁴ Qualified certificate means "A certificate which meets the requirements in Schedule 1 and is provided by a certification-service-provider who fulfils the requirements in Schedule 2."

¹⁰²⁵ Signatory means "A person who holds a signature-creation device and acts either on his own behalf or on behalf of the person he represents."

¹⁰²⁶ Signature creation data means, "Unique data (including, but not limited to, codes or private cryptographic keys) which are used by the signatory to create an electronic signature."

¹⁰²⁷ Signature creation device means, "Configured software or hardware used to implement the signature-creation data."

¹⁰²⁸ Signature-verification data means, "Data (including, but not limited to, codes or public cryptographic keys) which are used for the purpose of verifying an electronic signature."

¹⁰²⁹ Signature-verification device means "Configured software or hardware used to implement the signature-verification data."

¹⁰³⁰ Voluntary accreditation means, "means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned by the person charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the Certification service-provider is not entitled to exercise the rights stemming from the permission until he has received the decision of that person."

	United Kingdom and who issues qualified certificates to the public and which appears to her to be conduct detrimental to the interests of those persons who use or rely on those certificates with a view to making any of this evidence as she considers expedient available to the public in such manner as she considers appropriate.
Regulation 4(1)	<p>Where—</p> <p>(a) a certification-service-provider either—</p> <p>(i) issues a certificate as a qualified certificate to the public, or</p> <p>(ii) arantees a qualified certificate to the public,</p> <p>(b) a person reasonably relies on that certificate for any of the following matters—</p> <p>(i) he accuracy of any of the information contained in the qualified certificate at the time of issue,</p> <p>(ii) e inclusion in the qualified certificate of all the details referred to in Schedule 1,</p> <p>(iii) holding by the signatory identified in the qualified certificate at the time of its issue of the signature-creation data corresponding to the signature-verification data given or identified in the certificate, or</p> <p>(iv) he ability of the signature-creation data and the signature-verification data to be used in a complementary manner in cases where the certification-service provider generates them both,</p> <p>(c) hat person suffers loss as a result of such reliance, and</p> <p>(d) the certification-service-provider would be liable in damages in respect of any extent of the loss—</p> <p>(i) had a duty of care existed between him and the person referred to in subparagraph (b) above, and</p> <p>(ii) had the certification-service-provider been negligent, then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent unless the certification-service-provider proves that he was not negligent.</p>
Regulation 4(2)	For the purposes of the certification-service-provider's liability under paragraph (1) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (1)(b) above.
Regulation 4(3)	<p>Where—</p> <p>(a) certification-service-provider issues a certificate as a qualified certificate to the public,</p> <p>(b) person reasonably relies on that certificate,</p> <p>(c) hat person suffers loss as a result of any failure by the certification-service-provider to register revocation of the certificate, and</p> <p>(d) he certification-service-provider would be liable in damages in respect of any extent of the loss—</p> <p>(i) had a duty of care existed between him and the person referred to in subparagraph (b) above, and</p> <p>(ii) had the certification-service-provider been negligent, then that certification-service-provider shall be so liable to the same extent notwithstanding that there is no proof that the certification-service-provider was negligent unless the certification-service-provider proves that he was not negligent.</p>
Regulation 4(4)	For the purposes of the certification-service-provider's liability under paragraph (3) above there shall be a duty of care between that certification-service-provider and the person referred to in paragraph (3)(b) above.

Regulation 5(1)	A certification-service-provider who issues a certificate to the public and to whom this paragraph applies in accordance with paragraph (6) below— (a) shall not obtain personal data for the purpose of issuing or maintaining that certificate otherwise than directly from the data subject or after the explicit consent of the data subject, and (b) shall not process the personal data referred to in sub-paragraph (a) above— (i) to a greater extent than is necessary for the purpose of issuing or maintaining that certificate, or (ii) to a greater extent than is necessary for any other purpose to which the data subject has explicitly consented, unless the processing is necessary for compliance with any legal obligation, to which the certification-service-provider is subject, other than an obligation imposed by contract.
Regulation 5(2)	The obligation to comply with paragraph (1) above shall be a duty owed to any data subject who may be affected by a contravention of paragraph (1).
Regulation 5(3)	Where a duty is owed by virtue of paragraph (2) above to any data subject, any breach of that duty which causes that data subject to sustain loss or damage shall be actionable by him.
Regulation 5(4)	Compliance with paragraph (1) above shall also be enforceable by civil proceedings brought by the Crown for an injunction or for an interdict or for any other appropriate relief or remedy.
Regulation 5(5)	Paragraph (4) above shall not prejudice any right that a data subject may have by virtue of paragraph (3) above to bring civil proceedings for the contravention or apprehended contravention of paragraph (1) above.
Regulation 5(6)	Paragraph (1) above applies to a certification-service-provider in respect of personal data only if the certification-service-provider is established in the United Kingdom and the personal data are processed in the context of that establishment.
Regulation 5(7)	For the purposes of paragraph (6) above, each of the following is to be treated as established in the United Kingdom— (a) an individual who is ordinarily resident in the United Kingdom, (b) body incorporated under the law of, or in any part of, the United Kingdom, (c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and (d) any person who does not fall within sub-paragraph (a), (b) or (c) above but maintains in the United Kingdom— (i) an office, branch or agency through which he carries on any activity, or (ii) regular practice.

SCHEDULE 1: Requirements for Qualified Certificates

Qualified certificates must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established;
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;

- (h) the advanced electronic signature of the certification-service-provider issuing it;
 (i) limitations on the scope of use of the certificate, if applicable; and
 (j) limits on the value of transactions for which the certificate can be used, if applicable.

SCHEDULE 2: Requirements for Certification-Service-Providers Issuing Qualified Certificates

Certification-service-providers must:

- (a) demonstrate the reliability necessary for providing certification services;
 (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
 (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
 (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
 (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
 (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
 (g) take measures against forgery of certificates, and, in cases where the certification-service provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
 (h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
 (i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
 (j) not store or copy signature-creation data of the person to whom the certification-service provider provided key management services;
 (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;
 (l) use trustworthy systems to store certificates in a verifiable form so that:
- only authorised persons can make entries and changes,
 - information can be checked for authenticity,
 - certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained, and
 - any technical changes compromising these security requirements are apparent to the operator.

ANNEXURE Q: TRANSPOSITION OF THE E-MONEY DIRECTIVE INTO DOMESTIC REGULATION

Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions was transposed into domestic regulation by Ireland through the issuing of European Communities (Electronic Money) Regulations 2011. The Irish Regulation consists of 82 regulations. While all 82 regulations are important, the extracts below provide a summary of the most salient provisions for comparative purposes.¹⁰³¹

Table Q1: European Communities (Electronic Money) Regulations 2011

R 3(1)	Definitions	Several important terms are defined. These include: Agent: a person who provides payment services on behalf of an electronic money institution; Electronic money: electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which— (a) is issued on receipt of funds for the purpose of making payment transactions, (b) is accepted by a person other than the electronic money issuer, and (c) is not excluded by Regulation 5.
R 4(1)	Authority is the Central Bank	The Bank is the competent authority in the State for the purposes of the Electronic Money Directive. ¹⁰³²
R5	Electronic monetary value to which the Regulations do not apply	The Regulations do not apply to— (a) monetary value stored on instruments that can be used to acquire goods or services only— (i) in the premises used by the electronic money issuer, or (ii) under a commercial agreement with the electronic money issuer within a limited network of service providers or for a limited range of goods or services, or (b) monetary value that is used to make payment transactions executed by means of any telecommunication, digital or information technology device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or information technology device, on the condition that the telecommunication, digital or information technology operator does not act only as an intermediary between the electronic money user and the supplier of goods and services.
R6(1)	Persons that may issue electronic	A person shall not issue electronic money unless the person is— (a) a credit institution ¹⁰³³

¹⁰³¹ See the full regulation at: <http://www.irishstatutebook.ie/pdf/2011/en.si.2011.0183.pdf>

¹⁰³² In terms of Regulation 4(2), paragraph (1) does not imply that the Bank is required to supervise any business activity of an electronic money issuer other than those related to electronic money and the activities which fall within Regulation 28(1)(a) to (c).

¹⁰³³ Credit institution within the meaning of Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (including a branch, within the meaning of

	money	<p>(b) an electronic money institution ¹⁰³⁴</p> <p>(c) An Post in its capacity as an issuer of electronic money, or the postal authority of another Member State in its capacity as an issuer of electronic money,</p> <p>(d) the Bank, the European Central Bank or the central bank of another Member State, that is not acting in its capacity as a monetary authority, or other public authority,</p> <p>(e) a Member State, or a regional or local authority of a Member State, that is acting in its capacity as a public authority,</p> <p>(f) a credit union ¹⁰³⁵</p> <p>(g) a person that has been registered after qualifying as a small electronic money institution under Regulation 33,</p> <p>(h) a person for the time being permitted under Part 6 to issue electronic money, or</p> <p>(i) an electronic money institution authorised as such in another Member State pursuant to a law giving effect to the Electronic Money Directive.</p>
R5(2)	Bank must be given notice	An electronic money institution referred to in paragraph (1)(i) shall not, in the State, issue electronic money or provide a payment service unless the Bank has been given notice in accordance with Regulation 26.
R5(3)	May only issue E-Money in States covered by authorisation	An electronic money institution authorised under Chapter 2 to issue electronic money shall not, in the State or in another Member State, issue electronic money that is not covered by its authorisation.
R5(4)	E-Money institution authorised in another state may not provide a payment service not covered by authorisation	An electronic money institution authorised by the law of another Member State to issue electronic money shall not, in the State, issue electronic money or provide a payment service that is not covered by its authorisation.
R7	Bank to keep a register	The Bank shall maintain a public register (in these Regulations called "the Register") of— <p>(a) electronic money institutions and their agents and branches,</p> <p>(b) credit unions that have been approved to issue electronic money as an additional service under the Credit Union Act 1997, and</p> <p>(c) persons who have been registered after qualifying as a small electronic money institution under Regulation 33 and their agents and branches. ¹⁰³⁶</p>
R8	Applications for authorisation	An application for authorisation as an electronic money institution shall be in the form directed by the Bank and shall contain or be accompanied

point 3 of Article 4 of that Directive, located in a Member State of a credit institution having its head office in or, in accordance with Article 38 of that Directive, elsewhere than in a Member State).

¹⁰³⁴ As defined in Article 2 of the Electronic Money Directive.

¹⁰³⁵ Within the meaning of the Credit Union Act 15 of 1997.

¹⁰³⁶ In terms of Regulation 7(4), the Bank must make the Register publicly available for consultation and accessible online and is required to keep the Register up to date.

		<p>by—</p> <p>(a) programme of operations;</p> <p>(b) business plan;</p> <p>(c) evidence that the applicant holds initial capital;</p> <p>in the case of an applicant to which Regulations 29 and 30 apply, a description of the measures taken, in accordance with those Regulations, for protecting electronic money holders' funds;</p> <p>(e) a description of the applicant's governance arrangements and internal control mechanisms;</p> <p>(f) description of the internal control mechanisms that the applicant has established to comply with its obligations in relation to money laundering and terrorist financing and its obligations under <i>Regulation (EC) No. 1781/2006</i> of the European Parliament and of the Council of 15 November 20067 on information on the payer accompanying transfers of funds;</p> <p>(g) a description of the applicant's structural organisation, including, if applicable, a description of the intended use of agents and branches, a description of any outsourcing arrangements and a description of its participation in a national or international payment system;</p> <p>(h) the name of each person holding in the applicant, directly or indirectly, a qualifying holding;</p> <p>(i) the name of each director or other person responsible for the management of the applicant;</p> <p>(j) the name of the person who will carry out for the applicant the functions of audit required by the Companies Acts;</p> <p>(k) the applicant's legal status and memorandum and articles of association or other constitutional documents;</p> <p>(l) the address of the applicant's head office.</p>
R9(1)	Decision to grant or refuse authorisation	<p>The Bank may—</p> <p>(a) grant an authorisation to operate as an electronic money institution,</p> <p>(b) refuse to grant such an authorisation, or</p> <p>(c) grant such an authorisation subject to a specified condition or requirement.</p>
R9(2)	Proposed refusal of authorisation	<p>If the Bank proposes to refuse to grant authorisation as an electronic money institution, it shall give the applicant concerned notice in writing of its intention to refuse, setting out a statement of the reasons for the proposed refusal and specifying a period (not less than 21 calendar days) within which the applicant may make submissions in writing in relation to the proposed refusal.</p>
R10	Bank may require adjustments to applicant's business plan	<p>The Bank may, as a condition of granting an authorisation to an applicant, require the applicant to make a specified adjustment to the business plan submitted with its application. If the Bank requires such an adjustment to a business plan, references in these Regulations to the business plan are taken to be references to the plan as adjusted.</p>
R11	Conditions for granting of authorisation	<p>The Bank shall grant an authorisation only to—</p> <p>(a) legal person established in the State that has its head office and its registered office in the State, or</p> <p>(b) legal person which has a branch that is located in the State and whose head office is situated in a territory that is outside the European</p>

		Economic Area.
R13(1)	Initial capital	The Bank shall not authorise an applicant as an electronic money institution unless the applicant holds initial capital of at least €350,000 .
R13(2)	Calculation	For the purposes of calculating an applicant's initial capital, only the elements of its own funds described in subparagraphs (a) and (b) of Regulation 3(1) of the European Communities (Capital Adequacy of Credit Institutions) Regulations 2006 (S.I. No. 661 of 2006) shall be taken into account.
R13(3)	Own funds	The Bank shall not authorise an applicant as an electronic money institution unless the applicant holds own funds of at least— (a) the higher of— (i) the amount required by virtue of Regulation 13 as its initial capital, and (ii) the amount calculated— (I) in respect of the issuance of electronic money, by Method D, and (II) if it proposes to engage in payment services which are not related to the issuance of electronic money, by whichever of Methods A, B or C the Bank directs the institution, under Regulation 16(2), to use. (b) if the Bank so permits under paragraph (5), the amount required by virtue of Regulation 13 as the applicant's initial capital.
R13(4)	Bank may require institution to hold own funds that are 20% higher	On the basis of an evaluation of the risk-management processes, risk-loss database and internal control mechanisms of an electronic money institution, the Bank may require an applicant to hold an amount of own funds that is up to 20% higher than, or permit it to hold an amount of own funds that is up to 20% lower than, the amount that results from the application of the method directed by the Bank under Regulation 16(1) and, if applicable, Regulation 16(2).
R13(5)	Bank may permit an applicant not to hold own funds if certain conditions are met	The Bank may permit an applicant, on a case by case basis, not to hold own funds in accordance with paragraph (1)(a) if the electronic money institution is included in the consolidated supervision of a parent credit institution and meets the following conditions: (a) there is no current or foreseen material practical or legal impediment to the prompt transfer of own funds or repayment of liabilities by the parent credit institution; (b) either the parent credit institution satisfies the Bank regarding the prudent management of the electronic money institution and has declared, with the consent of the Bank, that it guarantees the commitments entered into by the electronic money institution, or the risks in the electronic money institution are of negligible interest; (c) the risk-evaluation, measurement and control procedures of the parent credit institution cover the electronic money institution; and (d) the parent credit institution holds more than 50% of the voting rights attaching to shares in the capital of the electronic money institution, or has the right to appoint or remove a majority of the members of the management body of the electronic money institution.
R15	Calculation of own funds — Method D	For Method D, the amount is at least 2% of the average outstanding electronic money.
R18	Maintenance of	Where any change affects the accuracy of information and evidence provided by

	authorisation	an electronic money institution in its application for authorisation in accordance with Regulation 8, the electronic money institution shall without undue delay inform the Bank in writing accordingly.
R19(1)	Audit and accounting	For supervisory purposes, an electronic money institution shall provide separate accounting information for activities other than the issuance of electronic money and payment services, and shall provide an auditor's report in relation to all such accounting information.
R20	Use of distributors, agents or any other entity acting on behalf of electronic money institution	<ul style="list-style-type: none"> • An electronic money institution may distribute or redeem electronic money through a distributor or agent. • An electronic money institution shall not issue electronic money through a distributor, agent or any other entity acting on its behalf. • An electronic money institution may engage a distributor or an agent to distribute or redeem electronic money in the exercise of its passport rights. • An electronic money institution may provide payment services in the State through an agent only if the agent is included on the Register. • An electronic money institution may provide payment services in the exercise • of its passport rights through an agent only if the agent is included on the Register.
R21(1)	Requirement for agents to be registered	<p>If an electronic money institution intends to provide payment services through an agent it shall, at least 30 calendar days before the agent commences to provide the service, notify the Bank in writing of the following:</p> <ul style="list-style-type: none"> • the name and address of the agent; • a description of the internal control mechanisms that will be used by • the agent to comply with the electronic money institution's obligations • in relation to money laundering and terrorist financing; • the names of directors and persons responsible for the management • of the agent; and • evidence that they are fit and proper persons.¹⁰³⁷
R21(6)	Agent to inform payment service users that it is acting on behalf of the E-Money institution	An electronic money institution shall ensure that any agent acting on its behalf informs payment service users that it is acting on behalf of the electronic money institution.
R22(2)	Outsourcing	If an electronic money institution intends to outsource an operational function of the issuance of electronic money or the provision of payment services, it shall notify the Bank in writing accordingly at least 30 calendar days before the outsourcing is to commence. ¹⁰³⁸

¹⁰³⁷ As per Regulation 21(2), when the Bank receives the information required by paragraph (1) it may list the agent in the Register. However, Regulation 21(3) states that, the Bank, before listing the agent in the Register, may, if it considers that the information provided to it is incorrect, take action to verify the information.

¹⁰³⁸ As per Regulation 22(1), an operational function is important if a defect or failure in its performance would materially impair— (a) the continuing compliance of the electronic money institution concerned with the requirements of its authorisation or its other obligations under these Regulations, (b) its financial performance, or (c) the soundness or continuity of its payment services.

R22(3)	Bank may direct E-Money institution not to outsource	<p>The Bank may direct an electronic money institution not to outsource an important operational function if the Bank is of the opinion that the outsourcing would—</p> <p>(a) result in the delegation by senior management of its responsibility,</p> <p>(b) alter the relationship and obligations of the electronic money institution towards its electronic money holders or payment service users under these Regulations,</p> <p>(c) undermine the conditions with which the electronic money institution is to comply in order to be authorised and remain so,</p> <p>(d) remove or modify any other condition of the electronic money institution's authorisation,</p> <p>(e) materially impair the quality of the electronic money institution's internal control, or</p> <p>(f) materially impair the ability of the Bank to monitor the electronic money institution's compliance with its obligations under the Regulations.</p>
R24	Liability when using third parties	<p>If an electronic money institution relies on a third party for the performance of an operational function, the electronic money institution shall take reasonable steps to ensure that the third party complies with the requirements of these Regulations so far as those requirements are capable of application to the third party.</p> <p>An electronic money institution remains fully liable for any acts of—</p> <p>(a) its employees, or</p> <p>(b) any distributor, agent, branch or entity to which activities are outsourced.</p>
R25	Record keeping	<p>An electronic money institution shall keep all appropriate records for the purpose of this Part for at least 5 years.</p>
R27	Withdrawal of authorisation	<p>The Bank may withdraw an authorisation issued to an electronic money institution under several circumstances including where the institution does not engage in the business of the issuance of electronic money, or the provision of payment services, in accordance with the authorisation within 12 months, expressly renounces the authorisation or ceases to engage in that business for more than 6 months, obtained the authorisation through false statements or any other irregular means, or would constitute a threat to the stability of the payment system by continuing its electronic money or payment services business.</p>
R28(1)	Additional activities in which electronic money institutions may engage	<p>Apart from the issuance of electronic money, an electronic money institution may engage in the following activities:</p> <ul style="list-style-type: none"> • the provision of payment services; • the granting of credit related to a payment service subject to paragraph (3); • the provision of operational and closely related ancillary services such as ensuring the execution of payment transactions, foreign exchange services, safekeeping activities, and the storage and processing of data, in respect of the issuance of electronic money or to the provision of payment services referred to in subparagraph (a); • the operation of payment systems referred to in point 6 of Article 4 of the Payment Services Directive and without prejudice to Article 28 of that Directive; • business activities other than issuance of electronic money and the provision

		of payment services.
R28(2)	Receipt of funds not deposit taking	The receipt of funds by an electronic money institution from an electronic money holder shall— <ul style="list-style-type: none"> • be exchanged for electronic money without delay, and • not constitute the taking of a deposit or other repayable funds.
R28(3)	May grant credit if conditions are met	An electronic money institution may grant credit related to a payment service referred to in point 4, 5 or 7 of Schedule 1 to the Payment Services Regulations only if the following conditions are met: <p>(a) the credit shall be ancillary and granted exclusively in connection with the execution of a payment transaction;</p> <p>(b) notwithstanding any law in relation to providing credit by means of credit cards, the credit shall be repaid within a short period that is not to be longer than 12 months;</p> <p>(c) credit shall not be granted from funds received or held for the purpose of executing a payment transaction; and</p> <p>(d) the own funds of the electronic money institution shall at all times and to the satisfaction of the Bank be appropriate in view of the overall amount of credit granted.</p>
R28(5)	May hold only payment accounts used exclusively for payment transactions	When an electronic money institution engages in the provision of one or more payment services that are not linked to the issuance of electronic money, it may hold only payment accounts used exclusively for payment transactions.
R28(6)	Funds received with a view to providing payment services are not deposits or E-Money	The receipt of funds by an electronic money institution with a view to the provision of a payment service does not constitute— <p>(a) the taking of a deposit or other repayable funds, or</p> <p>(b) electronic money.</p>
R29(2)	Safeguarding for electronic money institutions engaged in the issuance of electronic money	An electronic money institution that is engaged in the issuance of electronic money shall safeguard users' funds in either of the following ways: <p>(a) users' funds—</p> <p>(i) shall not be mixed at any time with the funds of any person other than the electronic money holder's on whose behalf the funds are held, and</p> <p>(ii) if still held by the electronic money institution and not yet delivered to the payee or transferred to another electronic money institution by the end of the business day after the day of receipt, shall be deposited in a separate account in a credit institution or invested in assets accepted by the Bank as secure and low-risk; or</p> <p>(b) users' funds shall be insured by an insurance company, or guaranteed by a credit institution, that does not belong to the same group as the electronic money institution, payable in the event that the electronic money institution is unable to meet its financial obligations, for an amount equal to that which would</p>

		have been segregated if the method set out in subparagraph (a) had been used. ¹⁰³⁹
R29(4)	No liquidator, creditor of E-Money institution has right to user's funds	No liquidator, receiver, administrator, examiner or creditor of an electronic money institution, nor the Official Assignee in Bankruptcy, has any recourse or right against users' funds held in accordance with paragraph (2)(a)(ii) received from electronic money holders or through a payment service provider until all proper claims of electronic money holders or of their heirs, successors or assigns against users' funds relating to such electronic money have been satisfied in full.
R30(2)	Safeguarding for electronic money institutions engaged in payment services not related to the issuance of electronic money	An electronic money institution that is engaged in payment services that are not related to the issuance of electronic money shall safeguard users' funds in either of the following ways: (a) users' funds— (i) shall not be mixed at any time with the funds of any person other than the payment service users on whose behalf the funds are held, and (ii) if still held by the electronic money institution and not yet delivered to the payee or transferred to another payment service provider by the end of the business day after the day of receipt, shall be deposited in a separate account in a credit institution or invested in assets accepted by the Bank as secure and low-risk; or (b) users' funds shall be insured by an insurance company, or guaranteed by a credit institution, that does not belong to the same group as the electronic money institution, payable in the event that the electronic money institution is unable to meet its financial obligations, for an amount equal to that which would have been segregated if the method set out in subparagraph (a) had been used.
R30(3)	No liquidator, receiver or administrator of an E-Money institution has recourse or rights against users funds	No liquidator, receiver, administrator, examiner or creditor of an electronic money institution, nor the Official Assignee in Bankruptcy, has any recourse or right against users' funds held in accordance with paragraph (2)(a)(ii) received from payment service users or through another payment service provider until all proper claims of payment service users or of their heirs, successors or assigns against users' funds relating to such payment services have been satisfied in full.
R33(1)	Definition of small electronic money institution	A person qualifies as a small electronic money institution for the purposes of these Regulations if— (a) the total business activities of the person immediately before the time of registration do not generate average outstanding electronic money that exceeds €1 million, and (b) the average amount of payment transactions executed by the person and any agent for which the person bears full responsibility during the previous 12 months, or the average amount of payment transactions likely to be executed by the person within the next 12 months, assessed on the projected total amount of payment transactions in its business plan, is not more than €3 million per month.

¹⁰³⁹ Regulation 29(3) states further that, "where an electronic money institution referred to in subparagraph (2) receives users' funds in the form of a payment instrument (a) such funds do not need to be safeguarded until they are credited to the electronic money institution's payment account or are otherwise made available to the institution, and (b) such funds shall be safeguarded by no later than 5 business days after the issuance of the electronic money concerned."

R33(2)	Registration of small E-Money institution and waiver of certain provisions	The Bank may waive the application to a person of all or part of the procedure and conditions set out in Chapters 2, 3, 4 and 6, and may register the person as a small electronic money institution, if— (a) he person satisfies the Bank that the person qualifies as a small electronic money institution, (b) none of the individuals responsible for the management or operation of the person's business has been convicted of any offence relating to money laundering or terrorist financing or any other financial crime, and (c) it has its head office in the State. ¹⁰⁴⁰
R33(4) & (5)	Small E-Money institution may engage in payment services but Bank may direct that they do not	(4) person registered as a small electronic money institution may engage in payment services not related to the issuance of electronic money which fall within Regulation 28(1), only if the conditions set out in Regulation 35 of the Payment Services Regulations are met to the satisfaction of the Bank. (5) The Bank may direct that a person registered as a small electronic money institution shall not engage in one or more of the activities which fall within Regulation 28(1).
R35	Requirement to apply for authorisation in certain circumstances	If a person registered as a small electronic money institution in accordance with Regulation 33 no longer qualifies as a small electronic money institution, or (in the case of a person subject to a direction under Regulation 33(5)) proposes to engage in a business activity other than the one specified in the relevant direction, the person shall apply for authorisation under Chapter 2 within 30 calendar days. (2) If a person referred to in paragraph (1) applies for authorisation in accordance with that paragraph, within the period of 30 calendar days referred to in that paragraph, it may continue issuing electronic money or providing a payment service until the Bank notifies it of its decision on the application. If such a person fails to apply for authorisation in accordance with that paragraph, it shall cease to issue electronic money or providing a payment service at the end of that period of 30 calendar days.
R38(1)	Restrictions on acquiring and disposing of qualifying holdings in electronic money institutions	38. (1) A proposed acquirer shall not, directly or indirectly, acquire a qualifying holding in an electronic money institution without having previously notified the Bank in writing of the intended size of the holding.
R39	Electronic money institution to provide information in relation to certain	(1) If an electronic money institution becomes aware of the acquisition of a qualifying holding in it, or an increase in the size of such a holding that results in the holding reaching or exceeding a prescribed percentage, the institution shall inform the Bank in writing of the acquisition or increase without delay. (2) If an electronic money institution becomes aware of a disposal of, or a

¹⁰⁴⁰ As per Regulation 33(3), a person registered as a small electronic money institution under paragraph (2) shall be taken to be an electronic money institution for the purposes of these Regulations except that— (a) its registration as a small electronic money institution is valid only in the State, and (b) it is not entitled to issue electronic money in any other Member State.

	acquisitions and disposals	reduction in the size of, a holding in it that results in the holding ceasing to be a qualifying holding or falling to or below a prescribed percentage, the institution shall inform the Bank in writing of the disposal or reduction without delay.
R42	Bank to cooperate with competent authorities of other Member States in certain cases	In carrying out its assessment of a proposed acquisition, the Bank shall work in full consultation with the relevant competent authorities of other Member States if the proposed acquirer concerned is— (a) an insurance undertaking, reinsurance undertaking, credit institution, investment firm or UCITS management company, or the market operator of a regulated market, authorised by a competent authority of another Member State, (b) the parent undertaking of such an undertaking, institution, firm, company or market operator, or (c) a person that controls such an undertaking, institution, firm, company or market operator.
R49	Electronic money institutions to provide information about shareholdings	An electronic money institution shall, at times specified by the Bank and at least once a year, notify the Bank of the names of shareholders or members who have qualifying holdings and the size of each such holding.
R52	Issuance and redeemability	An electronic money issuer must— (a) on receipt of funds, issue without delay electronic money at par value, and (b) at the request of the electronic money holder, redeem— (i) at any time, and (ii) at par value, the monetary value of the electronic money held.
R53	Conditions of redemption	An electronic money issuer must ensure— (a) that the contract between the electronic money issuer and the electronic money holder clearly and prominently states the conditions of redemption, including any fees relating to redemption, and (b) that the electronic money holder is informed of those conditions before being bound by any contract or offer.
R54	Fees for redemption	Redemption may be subject to a fee only where the fee is stated in the contract in accordance with Regulation 53(a), and— (a) redemption is requested before the termination of the contract, (b) the contract provides for a termination date and the electronic money holder terminates the contract before that date, or (c) redemption is requested more than one year after the date of termination of the contract. (2) Any such fees for redemption must be proportionate and commensurate with the costs actually incurred by the electronic money issuer.
R55	Amount of redemption	(1) Where before the termination of the contract an electronic money holder makes a request for redemption, the electronic money holder may request redemption of the monetary value of the electronic money in whole or in part, and the electronic money issuer must redeem the amount so requested subject to any fee imposed in accordance with Regulation 54. (2) (2) Where an electronic money holder makes a request for redemption on, or up to one year after, the date of the termination of the contract, the electronic

		<p>money issuer must redeem—</p> <p>(a) the total monetary value of the electronic money held, or</p> <p>(b) if the electronic money issuer carries out any business activities which fall within Regulation 28(1)(e) and it is not known in advance what proportion of funds received by it is to be used for electronic money, all the funds requested by the electronic money holder.</p>
R56	Redemption rights of persons other than consumers	Regulations 54 and 55 do not apply in the case of a person, other than a consumer, who accepts electronic money and, in such a case, the redemption rights of that person shall be subject to the contract between that person and the electronic money issuer.
R57	Prohibition of interest	<p>An electronic money issuer must not award—</p> <p>(a) interest in respect of the length of time during which the electronic money holder holds electronic money, or</p> <p>(b) any other benefit related to the length of time during which an electronic money holder holds electronic money.</p>
R59(1)	Supervision by Central Bank	<p>The Bank—</p> <p>(a) may require an electronic money issuer to provide such information as it requires to monitor the institution's compliance with these Regulations,</p> <p>(b) may carry out on-site inspections at—</p> <p>(i) the premises of an electronic money issuer,</p> <p>(ii) any distributor, agent or branch issuing electronic money or providing payment services under the responsibility of an electronic money issuer,</p> <p>(iii) premises of any entity to which an electronic money issuer's activities are outsourced, and</p> <p>(iv) any premises at which the issuance of electronic money or payment services are, or are suspected of being, conducted, and</p> <p>(c) may issue recommendations and guidelines.</p>
R59(2)	Bank may take steps to ensure that E-Money institution maintains sufficient capital	The Bank may take steps to ensure that an electronic money institution maintains sufficient capital for the issuance of electronic money or the provision of payment services, in particular where the activities not related to the issuance of electronic money of an electronic money institution impair or are likely to impair the financial soundness of the electronic money institution.
R60	Banks power to give directions	<p>If the Bank considers it necessary to do so in the interests of the proper and orderly supervision of the issuance of electronic money, the Bank may give a direction in writing to—</p> <p>(a) an electronic money institution,</p> <p>(b) another person registered to issue electronic money in the State, or</p> <p>(c) any other person involved in or connected with the issuance of electronic money in the State.</p> <p>(2) A direction under paragraph (1)—</p> <p>(a) takes effect on the date, or on the occurrence of the event, specified in the direction for the purpose, and</p> <p>(b) ceases to have effect on the earlier of—</p> <p>(i) the date, or the occurrence of the event, specified in the direction for the purpose, or</p>

		(ii) the expiration of the period of 12 months immediately following the day on which it took effect.
R61	Exchange of information	<p>(1) The Bank shall cooperate with the competent authorities of other Member States and with the European Central Bank and the central banks of other Member States and other relevant competent authorities designated under the laws of other Member States applicable to electronic money issuers.</p> <p>(2) The Bank may exchange information with—</p> <p>(a) the competent authorities of other Member States responsible for the authorisation and supervision of electronic money institutions,</p> <p>(b) the European Central Bank and the central banks of other Member States, in their capacity as monetary and oversight authorities, and, where appropriate, other public authorities responsible for overseeing payment and settlement systems, and</p> <p>(c) relevant authorities of other Member States designated under laws giving effect to the Electronic Money Directive and other acts of the European Communities applicable to electronic money issuers (for example, acts applicable to the protection of individuals with regard to the processing of personal data and to money laundering and terrorist financing).</p>
R63(1)	Power to appoint authorised officers	<p>The Bank may, in writing—</p> <p>(a) authorise a person as an authorised officer, and</p> <p>(b) evoke such an authorisation.</p>
R64(1)	Powers of authorised officers	<p>An authorised officer may, for the purpose of carrying out an investigation under this Part, do all or any of the following at any reasonable time during normal business hours—</p> <p>(a) enter any premises (other than a private dwelling) at which the officer has reasonable grounds to believe that the business of an electronic money issuer is, or has been, carried on, or on which there are relevant records,</p> <p>(b) search and inspect such premises and any relevant records on the premises,</p> <p>(c) secure for later inspection such premises or any part of such premises in which relevant records are kept or in which the officer has reasonable grounds for believing relevant records are kept,</p> <p>(d) require a person who carries on the business of an electronic money issuer and any person employed in connection with such a business to produce to the officer relevant records, and if any such record is in a non-legible form, to reproduce it in a legible form or to give the officer such information as the officer reasonably requires in relation to entries in the relevant records,</p> <p>(e) inspect and take copies of relevant records inspected or produced to the officer (including, in the case of information in a non-legible form, a copy of all or part of the information in a permanent legible form),</p> <p>(f) remove and retain any of the relevant records inspected or produced under this Act for such period as may be reasonable to allow their further examination,</p> <p>(g) require a person to give to the officer information (including information by way of a written report) that the officer reasonably requires in relation to</p>

		<p>activities covered by this Chapter and to produce to the officer any relevant records that the person has or has access to,</p> <p>(h) require a person by whom or on whose behalf data equipment is or has been used, or any person who has charge of, or is otherwise concerned with the operation of, the data equipment or any associated apparatus or material, to give the officer all reasonable assistance in relation the operation of that equipment, and</p> <p>(i) require a person to explain entries in any relevant records.¹⁰⁴¹</p>
R65(1)	Warrants	<p>If an authorised officer, while in the exercise of the authorised officer's powers under Regulation 64—</p> <p>(a) is prevented from entering any premises, or</p> <p>(b) believes that there are relevant records in a private dwelling, he or she may apply to a judge of the District Court for a warrant authorising the entry by the authorised officer into the premises or the dwelling.</p> <p>(2) If on an application under paragraph (1) a judge of the District Court is satisfied, on the information of the applicant authorised officer, that the applicant authorised officer—</p> <p>(a) as been prevented from entering the premises concerned, or</p> <p>(b) as reasonable grounds for believing that there are relevant records in the private dwelling concerned,</p> <p>the judge may issue a warrant under his or her hand authorising the applicant authorised officer, accompanied, if the judge considers it appropriate, by a specified number of members of the Garda Síochána, to enter, if need be by force, at any time within 4 weeks from the date of issue of the warrant, the premises or private dwelling and there exercise the powers set out in Regulation 64.</p>
R66	Out-of-Court complaint and redress procedures	<p>(1) The Financial Services Ombudsman has jurisdiction over the settlement of disputes between electronic money holders (being electronic money holders that are consumers or the operators of undertakings that were at the relevant time micro enterprises) and electronic money issuers concerning rights and obligations arising under these Regulations.</p> <p>(2) In the case of a cross-border dispute, the Financial Services Ombudsman shall cooperate actively with equivalent bodies in other European Economic Area Member States in resolving them.</p>
R67	Appealable decisions	<p>The following decisions of the Bank are appealable decisions for the purposes of Part VIIA of the Central Bank Act 1942:</p> <p>(a) a decision under Regulation 9—</p> <p>(i) refusing to grant an authorisation to operate as an electronic money institution, or</p> <p>(ii) anting such an authorisation subject to conditions or requirements;</p> <p>(b) decision under Regulation 27 to withdraw such an authorisation;</p> <p>(c) a decision under Regulation 33(5) or 78(3) to give a direction under that section to a person registered as a small electronic money institution;</p>

¹⁰⁴¹ Authorised officers are required to produce their certificates (Regulation 64(2)) and not enter a private dwelling (other than a part of the dwelling used as a place of work) except with the consent of the occupier (Regulation 64(3)).

		(d) a decision under Regulation 36 to withdraw a waiver granted under Regulation 33(2); (e) a decision under Regulation 60 to give a direction to a person; (f) a decision under Regulation 77(3) to revoke an authorisation granted under Regulation 77(2).
R68	Offence — operation as an electronic money institution without authorisation	A person commits an offence if the person contravenes any of paragraphs (1) to (6) of Regulation 6.
R69	Offence — false or misleading information in application	Without prejudice to the generality of Regulation 71, a person commits an offence if the person— (a) knowingly or recklessly makes a statement which is false or misleading in a material particular in an application for authorisation to operate as an electronic money institution, (b) knowingly or recklessly makes a statement which is false or misleading in a material particular to the Bank in relation to— (i) he obtaining of an authorisation to operate as an electronic money institution, or (ii) an approval, waiver or permission from the Bank concerning the operation of an electronic money institution, or (c) knowingly or recklessly provides information which is false or misleading in a material particular to the Bank in purported compliance with a requirement of or under Chapter 8 of Part 2.
R70	Offence — misappropriation of users' funds	70. A person who is a director, officer or employee of an electronic money institution commits an offence if he or she fraudulently misappropriates users' funds.
R71(1)	Offence — failure to keep appropriate records	A person who destroys, mutilates or falsifies, or is privy to the destruction, mutilation or falsification of, any record or document required under these Regulations, or makes or is privy to the making of a false entry therein, commits an offence. ¹⁰⁴²
R72	Offences — obstruction of authorised officer	A person who obstructs or interferes with an authorised officer in the exercise of the authorised officer's powers under these Regulations commits an offence. A person who, without reasonable excuse, refuses or fails to comply with a request or requirement of an authorised officer made in accordance with these Regulations commits an offence. A person commits an offence if the person knowingly or recklessly gives an authorised officer information which is false or misleading in a material particular.
R73	Offence — provision of false	An electronic money issuer commits an offence if the issuer, in purported compliance with a requirement under these Regulations—

¹⁰⁴² As per Regulation 71(2) it shall be a defense for a person prosecuted for an offence under paragraph (1) to prove that he or she had no intention to defeat the law. However, as per Regulation 71(3), a person who fraudulently disposes of, alters or makes an omission in any record or document referred to in paragraph (1), or who is privy to such disposal of, altering or making of an omission in any such record or document, commits an offence.

	or misleading information under these Regulations	(a) knowingly or recklessly provides an answer or explanation, makes a statement or produces information to the Bank that is false or misleading in a material particular, or (b) knowingly omits or withholds material information from the Bank.
R74	Penalties	A person who commits an offence under these Regulations is liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months or both, or (b) on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 3 years or both.

ANNEXURE R: TRANSPOSITION OF THE PSD INTO DOMESTIC LAW AND REGULATION

The PSD was transposed into national law by Gibraltar through the issuing of the Financial Service (EEA) (Payment Services) Regulations, 2010.¹⁰⁴³ The Regulations are transposed directly below for reference purposes.

Table R1: Financial Service (EEA) (Payment Services) Regulations, 2010

PART I: PRELIMINARY AND INTERPRETATION		
R2	Definitions	Several important terms are defined. These include: agent, authentication, branch, business day, competent authority, consumer, direct debit, durable medium, electronic money, framework contract, funds, micro-enterprise, money remittance, payee, payer, payment account, payment institution, payment order, payment service provider, payment service user, payment system, payment transaction, unique identifier and value date.
R3(1)	Scope – categories of payment service providers	These Regulations lay down rules distinguishing the following categories of payment service provider– (a) credit institutions within the meaning of the Financial Services (Banking) Act; (b) electronic money institutions within the meaning of the Financial Services (Banking) Act; (c) ost office giro institutions entitled by law to provide payment services; (d) ayment institutions within the meaning of these Regulations; (e) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities; (f) EEA States or their regional or local authorities when not acting in their capacity as public authorities. ¹⁰⁴⁴
R3(2)	Scope – transparency of conditions & information requirements for payment services, rights and obligations of payment service users	These Regulations lay down rules concerning transparency of conditions and information requirements for payment services, and the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services as a regular occupation or business activity.
R4(1)	Application – payment services	These Regulations apply to payment services provided in Gibraltar.

¹⁰⁴³ See <http://www.gibraltarlaws.gov.gi/articles/2010s078.pdf>

¹⁰⁴⁴ EEA States are interpreted in accordance with the provisions of the European Communities Act and a reference to an EEA State in these Regulations is deemed to include a reference to Gibraltar

	in Gibraltar	
R4(2)	Application – payment services with other EEA States	These Regulations apply to payment services provided as between Gibraltar and EEA States. However, with the exception of regulation 73, Parts III and IV apply only where both the payer’s payment service provider and the payee’s payment service provider are, or the sole payment service provider in the payment transaction is, located in Gibraltar or in an EEA State.
R4(3)	Application – Part III and IV apply to payment services made in Euro, Sterling or any other currency of an EEA State outside the Euro area	Parts III and IV apply to payment services made in Euro, Sterling, or any other currency of an EEA State outside the Euro area.
R4(4)	Minister may waive application of all / part of Regulations to post office & Savings Bank	The Minister may, by regulations, waive the application of all or part of the provisions of these Regulations to the post office and Gibraltar Savings Bank.
R4(5)	Regulations do not apply to the following	<p>These Regulations do not apply to any of the following–</p> <ul style="list-style-type: none"> (a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention; (b) payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee; (c) professional physical transport of banknotes and coins, including their collection, processing and delivery; (d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity; (e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services; (f) money exchange business, that is to say, cash-to-cash operations, where the funds are not held on a payment account; (g) payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee– <ul style="list-style-type: none"> (i) paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques; (ii) paper cheques similar to those referred to in sub paragraph (i) and governed by the laws of EEA States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques; (iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes; (iv) paper-based drafts similar to those referred to in sub paragraph (iii) and

		<p>governed by the laws of EEA States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;</p> <p>(v) paper-based vouchers;</p> <p>(vi) paper-based traveller's cheques; or</p> <p>(vii) paper-based postal money orders as defined by the Universal Postal Union;</p> <p>(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to regulation 28;</p> <p>(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in paragraph (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;</p> <p>(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (hereinafter referred to as "IT") and communication network provision, provision and maintenance of terminals and devices used for payment services;</p> <p>(k) services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;</p> <p>(l) payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;</p> <p>(m) payment transactions carried out between payment service providers, their agents or branches for their own account;</p> <p>(n) payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group; or</p> <p>(o) services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Schedule.</p>
PART II PAYMENT SERVICE PROVIDERS		
CHAPTER 1: PAYMENT INSTITUTIONS		
R5	Application for authorisation	An application for authorisation as a payment institution shall be submitted to the competent authority together with the following–

		<p>(a) a programme of operations setting out, in particular, the type of payment services envisaged;</p> <p>(b) a business plan including a forecast budget calculation for the first three financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;</p> <p>(c) evidence that the payment institution holds initial capital provided for in regulation 6;</p> <p>(d) for the payment institutions referred to in regulation 9(1), a description of the measures taken for safeguarding payment service users' funds in accordance with regulation 9;¹⁰⁴⁵</p> <p>(e) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, which demonstrates that these governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;</p> <p>(f) a description of the internal control mechanisms which the applicant has established in order to comply with obligations in relation to money laundering and terrorist financing under the Terrorism Act 2005, the Crime (Money Laundering and Proceeds) Act 2007 and Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds;</p> <p>(g) a description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of its participation in a national or international payment system;</p> <p>(h) the identity of persons holding in the applicant, directly or indirectly, qualifying holdings within the meaning of the Financial Services (Banking) Act, the size of their holdings and evidence of their suitability taking into account the need to ensure the sound and prudent management of a payment institution;</p> <p>(i) the identity of directors and persons responsible for the management of the payment institution and, where relevant, persons responsible for the management of the payment services activities of the payment institution, as well as evidence that they are of good repute and possess appropriate knowledge and experience to perform payment services as determined by the home EEA State of the payment institution;</p> <p>(j) where applicable, the identity of statutory auditors and audit firms as defined in the Financial Services (Auditors) Act 2009;</p> <p>(k) the applicant's legal status and memorandum and articles of association;</p> <p>(l) the address of the applicant's head office.</p>
R6	Initial capital ¹⁰⁴⁶	Payment institutions shall hold, at the time of authorisation, initial

¹⁰⁴⁵ For the purposes of sub-regulation (1)(d), (e) and (g), the applicant shall provide a description of its audit arrangements and the organisational arrangements it has set up with a view to taking all reasonable steps to protect the interests of its users and to ensure continuity and reliability in the performance of payment services.

¹⁰⁴⁶ Initial capital is defined in Regulation 6(2) as, "(a) capital, within the meaning of the Companies Act, in so far as it has been paid up, plus share premium accounts but excluding cumulative preferential shares; and (b) reserves, within the

		<p>capital as follows–</p> <p>(a) where the payment institution provides only the payment service listed in point 6 of the Schedule, its capital shall at no time be less than EUR 20,000;¹⁰⁴⁷</p> <p>(b) where the payment institution provides the payment service listed in point 7 of the Schedule, its capital shall at no time be less than EUR 50,000;¹⁰⁴⁸ and</p> <p>(c) where the payment institution provides any of the payment services listed in points 1 to 5 of the Schedule, its capital shall at no time be less than EUR 125,000.</p>
R7	Own funds	<p>(1) The own funds of payment institutions may not fall below the amount required under regulation 6 or 8, whichever is the higher.</p> <p>(2) The competent authority shall take the necessary measures to prevent the multiple use of elements eligible for own funds–</p> <p>(a) where the payment institution belongs to the same group as another payment institution, credit institution, investment firm, asset management company or insurance undertaking; or</p> <p>(b) where a payment institution has a hybrid character and carries out activities other than providing payment services listed in the Schedule.</p> <p>(3) If the conditions laid down in sub-regulation (4) are met, the competent authority may choose not to apply regulation 8 to payment institutions which are included in the consolidated supervision of the parent credit institution pursuant to the Financial Services (Banking) Act.</p> <p>(4) The conditions to which sub-regulation (3) refers are as follows–</p> <p>(a) the payment institution must be a subsidiary of a credit institution, where both the subsidiary and the credit institution are subject to authorisation and supervision by the Financial Service Commission, and the subsidiary is included in the supervision on a consolidated basis of the credit institution which is the parent undertaking, and the requirements of this sub-regulation are satisfied, in order to ensure that own funds are distributed adequately among the parent undertaking and the subsidiaries;</p> <p>(b) there must be no current or foreseen material, practical or legal impediment to the prompt transfer of own funds or repayment of liabilities by the parent undertaking of the payment institution;</p> <p>(c) either the parent undertaking satisfies the competent authority regarding the prudent management of the subsidiary and has declared, with the consent of the competent authority, that it guarantees the commitments entered into by the subsidiary, or the risks in the subsidiary are of negligible interest;</p> <p>(d) the risk evaluation, measurement and control procedures of the parent undertaking cover the subsidiary; and</p> <p>(e) the parent undertaking holds more than 50 % of the voting rights attaching to shares in the capital of the subsidiary or has the right to appoint or remove a majority of the members of the management body of the subsidiary.</p>

meaning of the Companies Act and profits and losses brought forward as a result of the application of the final profit or loss.”

¹⁰⁴⁷ Money remittance

¹⁰⁴⁸ Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

		(5) For the purposes of this regulation, "own funds" is to be construed in accordance with the provisions of the Financial Services (Banking) Act.
R8	Calculation of own funds	<p>8.(1) Notwithstanding the initial capital requirements set out in regulation 6, the competent authority shall require payment institutions to hold, at all times, own funds calculated in accordance with one of the following three methods as the competent authority may see fit.</p> <p>a) Method A The payment institutions own funds shall amount to at least 10 % of its fixed overheads of the preceding year. The competent authorities may adjust that requirement in the event of a material change in a payment institution's business since the preceding year. Where a payment institution has not completed a full year's business at the date of the calculation, the requirement shall be that its own funds amount to at least 10 % of the corresponding fixed overheads as projected in its business plan, unless an adjustment to that plan is required by the competent authority.</p> <p>(b) Method B The payment institution's own funds shall amount to at least the sum of the following elements multiplied by the scaling factor "k" defined in sub-regulation (2), where payment volume (hereinafter "PV") represents one twelfth of the total amount of payment transactions executed by the payment institution in the preceding year:</p> <p>(i) 4,0 % of the slice of PV up to EUR 5 million; plus (ii) ,5 % of the slice of PV above EUR 5 million up to EUR 10 million; plus (iii) % of the slice of PV above EUR 10 million up to EUR 100 million; plus (iv) 0,5 % of the slice of PV above EUR 100 million up to EUR 250 million; plus (v) 0,25 % of the slice of PV above EUR 250 million.</p> <p>c) Method C The payment institution's own funds shall amount to at least the relevant indicator defined in point (a), multiplied by the multiplication factor defined in point (b) and by the scaling factor "k" defined in sub-regulation (2). (a) The relevant indicator is the sum of the following – (i) interest income; (ii) interest expenses; (iii) commissions and fees received; and (iv) other operating income. Each element shall be included in the sum with its positive or negative sign. Income from extraordinary or irregular items may not be used in the calculation of the relevant indicator. Expenditure on the outsourcing of services rendered by third parties may reduce the relevant indicator if the expenditure is incurred from an undertaking subject to supervision under these Regulations. The relevant indicator is calculated on the basis of the twelve-monthly observation at the end of the previous financial year. The relevant indicator shall be calculated over the previous financial year. Nevertheless own funds calculated</p>

		<p>according to Method C shall not fall below 80 % of the average of the previous three financial years for the relevant indicator. When audited figures are not available, business estimates may be used.</p> <p>(b) The multiplication factor shall be–</p> <p>(i) 10 % of the slice of the relevant indicator up to EUR 2,5 million;</p> <p>(ii) 8 % of the slice of the relevant indicator from EUR 2,5 million up to EUR 5 million;</p> <p>(iii) 6 % of the slice of the relevant indicator from EUR 5 million up to EUR 25 million;</p> <p>(iv) 3 % of the slice of the relevant indicator from EUR 25 million up to 50 million;</p> <p>(v) 1,5 % above EUR 50 million.</p> <p>(2) The scaling factor “k” to be used in Methods B and C shall be as follows –</p> <p>(a) 0,5 where the payment institution provides only the payment service listed in point 6 of the Schedule;</p> <p>(b) 0,8 where the payment institution provides the payment service listed in point 7 of the Schedule;</p> <p>(c) 1 where the payment institution provides any of the payment services listed in paragraphs 1 to 5 of the Schedule.</p> <p>(3) Based on an evaluation of the risk-management processes, risk loss data base and internal control mechanisms of the payment institution, the competent authority may –</p> <p>(a) require the payment institution to hold an amount of own funds which is up to 20 % higher than the amount which would result from the application of the method chosen in accordance with sub-regulation (1); or</p> <p>(b) permit the payment institution to hold an amount of own funds which is up to 20 % lower than the amount which would result from the application of the method chosen in accordance with sub-regulation (1).</p>
R9	Safeguarding requirements	<p>9.(1) The competent authority shall require a payment institution which provides any of the payment services listed in the Schedule and, at the same time, is engaged in other business activities referred to in regulation 16(1)(c) to safeguard funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions, as follows –</p> <p>(a) either –</p> <p>(i) they shall not be commingled at any time with the funds of any natural or legal person other than payment service users on whose behalf the funds are held and, where they are still held by the payment institution and not yet delivered to the payee or transferred to another payment service provider by the end of the business day following the day when the funds have been received, they shall be deposited in a separate account in a credit institution or invested in secure, liquid low-risk assets as defined by the competent authority; and</p> <p>(ii) they shall be insulated in accordance with Gibraltar laws in the interest of the payment service users against the claims of other creditors of the payment</p>

		<p>institution, in particular in the event of insolvency; or (b) they shall be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which would have been segregated in the absence of the insurance policy or other comparable guarantee, payable in the event that the payment institution is unable to meet its financial obligations</p> <p>(2) Where— (a) a payment institution is required to safeguard funds under sub-regulation (1) and a portion of those funds is to be used for future payment transactions with the remaining amount to be used for non-payment services, that portion of the funds to be used for future payment transactions shall also be subject to the requirements under sub-regulation (1); and (b) the portion referred to in paragraph (a) is variable or unknown in advance, the competent authority may allow payment institutions to apply this sub-regulation on the basis of a representative portion assumed to be used for payment services provided such a representative portion can be reasonably estimated on the basis of historical data to the satisfaction of the competent authority. (3) The Minister may, by regulations, require that payment institutions which are not engaged in other business activities referred to in regulation 16(1)(c) shall also comply with the safeguarding requirements under sub-regulation (1). (4) The Minister may, by regulations, also limit the safeguarding requirements under sub-regulation (1), to funds of those payment service users whose funds individually exceed a threshold of EUR 600.</p>
R10	Granting of authorisation	<p>10.(1) The competent authority shall require undertakings other than those referred to in regulation 3(1)(a) to (c), (e) and (f) and other than legal or natural persons benefiting from a waiver under regulation 26, who intend to provide payment services, to obtain authorisation as a payment institution before commencing the provision of payment services. An authorisation shall be granted by the competent authority only to a legal person established in Gibraltar.</p> <p>(2) An authorisation shall be granted if the information and evidence accompanying the application complies with all the requirements under regulation 5 and if the competent authority's overall assessment, having scrutinised the application, is favourable. Before an authorisation is granted, the competent authority may, where relevant, consult relevant public authorities.</p> <p>(3) A payment institution which under Gibraltar law or the national law of its home EEA State is required to have a registered office, shall have its head office in the same place as its registered office.</p> <p>(4) The competent authority shall grant an authorisation only if, taking into account the need to ensure the sound and prudent management of a payment institution, the payment institution has robust governance arrangements for its payment services business, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective</p>

		<p>procedures to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures; those arrangements, procedures and mechanisms shall be comprehensive and proportionate to the nature, scale and complexity of the payment services provided by the payment institution.</p> <p>(5) Where a payment institution provides any of the payment services listed in the Schedule and, at the same time, is engaged in other business activities, the competent authority may require the establishment of a separate entity for the payment services business, where the non-payment services activities of the payment institution impair or are likely to impair either the financial soundness of the payment institution or the ability of the competent authority to monitor the payment institution's compliance with all obligations in these Regulations.</p> <p>(6) The competent authority shall refuse to grant an authorisation if, taking into account the need to ensure the sound and prudent management of a payment institution, it is not satisfied as to the suitability of the shareholders or members that have qualifying holdings.</p> <p>(7) Where close links exist between the payment institution and other natural or legal persons, the competent authority shall grant an authorisation only if those links do not prevent the effective exercise of its supervisory functions.</p> <p>(8) The competent authority shall grant an authorisation only if the laws, regulations or administrative provisions of a third country governing one or more natural or legal persons with which the payment institution has close links, or difficulties involved in the enforcement of those laws, regulations or administrative provisions, do not prevent the effective exercise of its supervisory functions.</p> <p>(9) In accordance with the provisions of the Directive, an authorisation under these Regulations shall be valid in all EEA States and shall allow the payment institution concerned to provide payment services throughout the EEA, either under the freedom to provide services or the freedom of establishment, provided that such services are covered by the authorisation.</p> <p>(10) In this regulation, "close links" means a situation in which two or more natural or legal persons are linked in any of the following ways –</p> <p>(a) participation in the form of ownership, direct or by way of control, of 20 % or more of the voting rights or capital of an undertaking;</p> <p>(b) control relationship; or</p> <p>(c) the fact that both or all are permanently linked to one and the same third person by a control relationship.</p>
R11	Communication of the decision	<p>11. Within three months of receipt of an application or, should the application be incomplete, of all the information required for the decision, the competent authority shall inform the applicant whether the authorisation has been granted or refused. Reasons shall be given whenever an authorisation is refused.</p>
R12	Withdrawal of authorisation	<p>12.(1) The competent authority may withdraw an authorisation issued to a payment institution only where the institution–</p> <p>(a) does not make use of the authorisation within 12 months, expressly renounces the authorisation or has ceased to engage in business for more than</p>

		<p>six months;</p> <p>(b) has obtained the authorisation through false statements or any other irregular means;</p> <p>(c) no longer fulfills the conditions for granting the authorisation;</p> <p>(d) would constitute a threat to the stability of the payment system by continuing its payment services business; or</p> <p>(e) falls within one of the other cases where Gibraltar laws provide for withdrawal of an authorisation.</p> <p>(2) Reasons shall be given for any withdrawal of an authorisation and those concerned shall be informed accordingly.</p> <p>(3) Notice of the withdrawal of an authorisation shall be published by the competent authority and in the Gazette.</p>
R13	Registration	<p>13.(1) There shall be a public register, in such form as the Minister may deem appropriate, where there shall be entered the details of authorised payment institutions, their agents and branches, as well as of natural and legal persons, their agents and branches, benefiting from a waiver under regulation 26, and of the institutions referred to in regulation 4 that are entitled to provide payment services.</p> <p>(2) The register shall identify the payment services for which the payment institution is authorised or for which the natural or legal person has been registered.</p> <p>(3) Authorised payment institutions shall be listed in the register separately from natural and legal persons that have been registered in accordance with regulation 26.</p> <p>(4) The register shall be publicly available for consultation, accessible online, and updated on a regular basis.</p>
R14	Maintenance of authorisation	<p>14. Where any change affects the accuracy of information and evidence provided in accordance with regulation 5, the payment institution shall, without undue delay, inform the competent authority accordingly.</p>
R15	Accounting and statutory audit	<p>5.(1) The following legislation applies to payment institutions–</p> <p>(a) the Financial Services (Auditors) Act 2009;</p> <p>(b) the Companies (Accounts) Act 1999;</p> <p>(c) the Companies (Consolidated Accounts) Act 1999;</p> <p>(d) the Banking (Accounts Directive) Regulations 1997;</p> <p>(e) the Insurance Companies (Accounts Directive) Regulations 1997; and</p> <p>(f) Regulation (EC) 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of international accounting standards.</p> <p>(2) Unless exempted under any legislation referred to in sub-regulation</p> <p>(1), the annual accounts and consolidated accounts of payment institutions shall be audited by statutory auditors or audit firms within the meaning of Financial Services (Auditors) Act 2009.</p> <p>(3) For supervisory purposes, the competent authority shall require that payment institutions provide separate accounting information for payment</p>

		<p>services listed in the Schedule and activities referred to in regulation 16(1), which shall be subject to an auditor's report. That report shall be prepared, where applicable, by the statutory auditors or an audit firm.</p> <p>(4) Provisions in the Financial Services (Banking) Act relating to reports to the competent authority under sections 46 to 47 of the Financial Services (Banking) Act, shall apply to the statutory auditors or audit firms of payment institutions in respect of payment services activities.</p>
R16	Activities	<p>16(1) Apart from the provision of payment services listed in the Schedule, payment institutions shall be entitled to engage in the following activities–</p> <p>(a) the provision of operational and closely related ancillary services such as ensuring the execution of payment transactions, foreign exchange services, safekeeping activities, and the storage and processing of data;</p> <p>(b) the operation of payment systems, without prejudice to regulation 28;</p> <p>(c) business activities other than the provision of payment services, having regard to applicable European Union and Gibraltar law.</p> <p>(d) the own funds of the payment institution shall at all times and to the satisfaction of the supervisory authorities be appropriate in view of the overall amount of credit granted.</p> <p>(4) Payment institutions shall not conduct the business of taking deposits or other repayable funds within the meaning of the Financial Services (Banking) Act.</p> <p>(5) These Regulations shall be without prejudice to any statutory provision relating to consumer credit or the conditions for granting credit to consumers that is in conformity with European Union law.</p>
R17	Use of agents, branches or entities to which activities are outsourced	<p>17(1) When a payment institution intends to provide payment services through an agent, it shall communicate the following information to the competent authority–</p> <p>(a) the name and address of the agent;</p> <p>(b) a description of the internal control mechanisms that will be used by agents in order to comply with the obligations in relation to money laundering and terrorist financing under the Terrorism Act 2005 and the Crime (Money Laundering and Proceeds) Act 2007; and</p> <p>(c) the identity of directors and persons responsible for the management of the agent to be used in the provision of payment services and evidence that they are fit and proper persons.</p> <p>(2) When the competent authority receives the information set out in subregulation (1) then it may list the agent in the register provided for in regulation 13.</p> <p>(3) Before listing the agent in the register, the competent authority may, if it considers that the information provided is incorrect, take further action to verify the information.</p> <p>(4) If, after taking action to verify the information, the competent authority is not satisfied that the information provided to it pursuant to subregulation (1) is correct, it shall refuse to list the agent in the register provided for in regulation 13.</p> <p>(5) Where a payment institution wishes to provide payment services in an EEA State by engaging an agent, it shall follow the procedures set out in regulation</p>

		<p>25. In that case, before the agent may be registered under this regulation, the competent authority shall inform the competent authorities of the host EEA State of its intention to register the agent and take their opinion into account.</p> <p>(6) Where the competent authority has reasonable grounds to suspect, in particular, as a result of any information provided or opinion given by the competent authorities in the host EEA State, that, in connection with the intended engagement of the agent or establishment of the branch, money laundering or terrorist financing is taking place, has taken place or been attempted, or that the engagement of such agent or establishment of such branch could increase the risk of money laundering or terrorist financing, it may refuse to register the agent or branch, or may withdraw the registration, if already made, of the agent or branch.</p> <p>(7) Where a payment institution intends to outsource operational functions of payment services, it shall inform the competent authority accordingly.</p> <p>(8) Outsourcing of important operational functions may not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authority to monitor the payment institution's compliance with all obligations laid down in these Regulations.</p> <p>(9) For the purposes of this sub-regulation (8), an operational function shall be regarded as important if a defect or failure in its performance would materially impair any of the following–</p> <p>(a) the continuing compliance of a payment institution with the requirements of its authorisation requested under this Part;</p> <p>(b) the continuing compliance of a payment institution with its other obligations under these Regulations;</p> <p>(c) the payment institution's financial performance; or</p> <p>(d) the soundness or the continuity of the payment institution's payment services.</p> <p>(10) The competent authority shall ensure that when payment institutions outsource important operational functions, the payment institutions comply with the following conditions:</p> <p>(a) the outsourcing shall not result in the delegation by senior management of its responsibility;</p> <p>(b) the relationship and obligations of the payment institution towards its payment service users under these Regulations shall not be altered;</p> <p>(c) the conditions with which the payment institution is to comply in order to be authorised and remain so in accordance with this Part shall not be undermined; and</p> <p>(d) none of the other conditions subject to which the payment institution's authorisation was granted shall be removed or modified.</p> <p>(11) Payment institutions shall ensure that agents or branches acting on their behalf inform payment service users of this fact.</p>
R18	Liability	<p>18(1) The competent authority shall ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of these Regulations are complied with.</p>

		(2) The competent authority shall require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced.
R19	Record keeping	Payment institutions shall keep all appropriate records for the purpose of this Part for at least five years.
R20	Designation of a person to be competent authority	<p>20(1) The Minister shall designate either a public authority, or a body expressly empowered by statute for the purpose, as the competent authority responsible for the authorisation and prudential supervision of payment institutions which is to carry out the duties provided for under this Part.</p> <p>(2) The competent authority shall be independent from economic bodies and shall avoid conflicts of interest. Without prejudice to sub-regulation (1), payment institutions, credit institutions, electronic money institutions, or post office giro institutions shall not be designated as competent authority.</p> <p>(3) The Minister shall ensure the European Commission is informed of the designation accordingly.</p> <p>(4) The Minister may make regulations under the principal Act to ensure that the competent authority possesses all the powers necessary for the performance of its duties under these Regulations.</p> <p>(5) Sub-regulation (1) shall not imply that the competent authority is required to supervise business activities of the payment institutions other than the provision of payment services listed in the Schedule and the activities listed in regulation 16(1)(a).</p>
R21	Supervision	<p>21(1) The controls exercised by the competent authority for checking continued compliance with this Part shall be proportionate, adequate and responsive to the risks to which payment institutions are exposed, and in order to check compliance with this Part, the competent authority shall be entitled to take the following steps, in particular–</p> <p>(a) to require the payment institution to provide any information needed to monitor compliance;</p> <p>(b) to carry out on-site inspections at the payment institution, at any agent or branch providing payment services under the responsibility of the payment institution, or at any entity to which activities are outsourced;</p> <p>(c) to issue recommendations, guidelines and, if applicable, binding administrative provisions; and</p> <p>(d) to suspend or withdraw authorisation in cases referred to in regulation 12.</p> <p>(2) Without prejudice to the procedures for the withdrawal of authorisations and the provisions of criminal law, the competent authority may, in respect of the persons listed in sub-regulation (3), adopt or impose such penalties or measures aimed specifically at ending observed breaches or the causes of such breaches as are reasonable in the circumstances, taking all relevant considerations into account.</p> <p>(3) Those persons are payment institutions, or those who effectively control the business of payment institutions, which breach laws, regulations or administrative provisions concerning the supervision or pursuit of their payment service business.</p> <p>(4) Notwithstanding the requirements of regulations 6, 7(1) and (2) and 8, the competent authority is entitled to take such steps described under</p>

		subregulation (1) as are reasonable to ensure sufficient capital for payment services, in particular where the non-payment services activities of the payment institution impair or are likely to impair the financial soundness of the payment institution.
R22	Professional secrecy	<p>22(1) All persons working or who have worked for the competent authority, as well as experts acting on behalf of the competent authority, are bound by the obligation of professional secrecy, without prejudice to cases covered by criminal law.</p> <p>(2) In the exchange of information carried out pursuant to regulation 24, professional secrecy shall be strictly applied to ensure the protection of individual and business rights.</p> <p>(3) When applying this regulation, account shall be taken of the provisions of Schedule 3 of the Financial Services (Banking) Act.</p>
R23	Right to apply to the supreme court	<p>23(1) Decisions taken by the competent authority in respect of a payment institution pursuant to these Regulations may be contested before the Supreme Court.</p> <p>(2) Sub-regulation (1) shall apply also in respect of a failure to act.</p>
R24	Exchange of information	<p>24(1) The competent authority shall cooperate with the competent authorities of the EEA States and, where appropriate, with the European Central Bank, the national central banks of the EEA States and other relevant competent authorities designated by EEA States as having responsibilities in respect of payment service providers.</p> <p>(2) Information shall also be exchanged between the competent authority and the following–</p> <p>(a) the competent authorities of EEA States responsible for the authorisation and supervision of payment institutions;</p> <p>(b) the European Central Bank and the national central banks of EEA States, in their capacity as monetary and oversight authorities, and, where appropriate, other public authorities responsible for overseeing payment and settlement systems;</p> <p>(c) other relevant authorities designated by laws applicable to payment service providers, such as laws applicable to the protection of individuals with regard to the processing of personal data as well as money laundering and terrorist financing.</p>
R25	Exercise of the right of establishment and freedom to provide services	<p>25(1) Any authorised payment institution wishing to provide payment services for the first time in a EEA State other than Gibraltar, in exercise of the right of establishment or the freedom to provide services, shall so inform the competent authority.</p> <p>(2) Within one month of receiving that information, the competent authority shall inform the competent authorities of the host EEA State of the name and address of the payment institution, the names of those responsible for the management of the branch, its organisational structure and of the kind of payment services it intends to provide in the territory of the host EEA State.</p> <p>(3) The competent authority shall cooperate with the competent authorities of the host EEA State in order to carry out the controls and take the necessary steps provided for in regulation 21 in respect of the agent, branch or entity to</p>

		<p>which a payment institution has outsourced activities.</p> <p>(4) By way of cooperation in accordance with this regulation, the competent authority shall notify the competent authorities of the host EEA State whenever it intends to carry out an on-site inspection in the territory of the latter.</p> <p>(5) The competent authority may delegate to the competent authorities of the host EEA State the task of carrying out on-site inspections of the institution concerned.</p> <p>(6) The competent authority shall provide the competent authorities of the host EEA State with all essential or relevant information, in particular, in the case of infringements or suspected infringements by an agent, a branch or an entity to which activities are outsourced. In this regard, the competent authority shall communicate to the competent authorities of other States, upon request, all relevant information and, on its own initiative, all essential information.</p> <p>(7) This regulation is without prejudice to the obligation of competent authorities to supervise or monitor compliance with other financial services legislation.</p>
R26	Conditions	<p>26(1) Notwithstanding regulation 13, the Minister may waive or allow the competent authority to waive the application of all or part of the procedure and conditions set out in regulations 5 to 25, with the exception of regulations 20, 22, 23 and 24, and allow natural or legal persons to be entered in the register provided for in regulation 13, where—</p> <p>(a) the average of the preceding 12 months' total amount of payment transactions executed by the person concerned, including any agent for which it assumes full responsibility, does not exceed EUR 3 million per month. That requirement shall be assessed on the projected total amount of payment transactions in its business plan, unless an adjustment to that plan is required by the competent authority; and</p> <p>(b) none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes.</p> <p>(2) Any natural or legal person registered in accordance with subregulation (1) carrying on business in Gibraltar shall be required to have its head office or place of residence in Gibraltar.</p> <p>(3) The persons referred to in sub-regulation (1) shall be treated as payment institutions, save that regulations 10(9) and 25 shall not apply to them.</p> <p>(4) The Minister may make regulations under the principal Act to provide that any natural or legal person registered in accordance with sub-regulation (1) may engage only in certain activities listed in regulation 16.</p> <p>(5) The persons referred to in sub-regulation (1) shall notify the competent authority of any change in their situation which is relevant to the conditions specified in that sub-regulation, and where the conditions set out in the preceding sub-regulations are no longer fulfilled, the persons concerned shall seek authorisation from the competent authority within 30 calendar days in accordance with the procedure laid down in regulation 10.</p> <p>(6) This regulation shall not be applied in respect of provisions relating</p>

		money-laundering or the financing of terrorism.
R27	Notification and information	<p>27.(1) Where the right to a waiver, or any subsequent changes thereto, is exercised pursuant to regulation 26, the Minister shall ensure the European Commission is notified forthwith.</p> <p>(2) The Minister shall ensure the European Commission is informed of the number of natural and legal persons concerned and, on an annual basis, of the total amount of payment transactions executed as of 31 December of each calendar year, as referred to in regulation 26(1)(a).</p>
CHAPTER II COMMON PROVISIONS		
R28	Access to payment systems	<p>28(1) The procedures and practices relating to the access of authorised or registered payment service providers that are legal persons to payment systems shall be objective, non-discriminatory and proportionate and do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system.</p> <p>(2) Payment systems shall not impose on payment service providers, on payment service users or on other payment systems any of the following requirements—</p> <p>(a) any restrictive rule on effective participation in other payment systems;</p> <p>(b) any rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; or</p> <p>(c) any restriction on the basis of institutional status.</p> <p>(3) Sub-regulations (1) and (2) shall not apply to—</p> <p>(a) payment systems designated under the Financial Markets and Insolvency (Settlement Finality) Regulations 2002;</p> <p>(b) payment systems composed exclusively of payment service providers belonging to a group composed of entities linked by capital where one of the linked entities enjoys effective control over the other linked entities; or</p> <p>(c) payment systems where a sole payment service provider (whether as a single entity or as a group)—</p> <p>(i) acts or can act as the payment service provider for both the payer and the payee and is exclusively responsible for the management of the system; and</p> <p>(ii) licenses other payment service providers to participate in the system and the latter have no right to negotiate fees between or amongst themselves in relation to the payment system although they may establish their own pricing in relation to payers and payees.</p>
R29	Prohibition for persons other than payment service providers to provide payment services	<p>29. It shall be an offence for natural or legal persons that are neither payment service providers nor explicitly excluded from the scope of these Regulations to provide the payment services listed in the Schedule.</p>
PART III TRANSPARENCY OF CONDITIONS AND INFORMATION REQUIREMENTS FOR PAYMENT SERVICES		
CHAPTER I GENERAL RULES		
R30	Scope of part	30(1) This Part shall apply to single payment transactions, framework contracts

		<p>and payment transactions covered by them, and parties may agree that it shall not apply in whole or in part when the payment service user is not a consumer.</p> <p>(2) The Minister may, by regulations under the principal Act, provide that the provisions in this Part shall be applied to micro enterprises in the same way as to consumers.</p> <p>(3) These Regulations shall be without prejudice to any statutory provision relating to consumer credit or the conditions for granting credit to consumers that is in conformity with European Union law.</p>
R31	Other provisions in European Union legislation	<p>31(1) The provisions of this Part are without prejudice to any statutory provision containing additional requirements on prior information.</p> <p>(2) Where the provisions of the Financial Services (Distance Marketing) Act 2006 apply, the information requirements set out in Schedule 1 paragraph 1, with the exception of paragraphs 2(c) to (g), 3(a), (d) and (e), and 4(b) of that Act, shall be replaced by regulations 36, 37, 41 and 42 of these Regulations.</p>
R32	Charges for information	<p>32(1) The payment service provider shall not charge the payment service user for providing information under this Part.</p> <p>(2) A payment service provider and a payment service user may agree on charges for additional or more frequent information, or transmission by means of communication other than those specified in the framework contract, provided at the payment service user's request.</p> <p>(3) Where a payment service provider may impose charges for information in accordance with sub-regulation (2), the charges shall be appropriate and in line with the payment service provider's actual costs.</p>
R33	Burden of proof on information requirements	<p>33. The Minister may, by regulations under the principal Act, stipulate that the burden of proof shall lie with the payment service provider to prove that it has complied with the information requirements set out in this Part.</p>
R34	Derogation from information requirements for low-value payment instruments and electronic money	<p>34.(1) In cases of payment instruments which, according to the framework contract, concern only individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time—</p> <p>(a) by way of derogation from regulations 41, 42 and 46, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed to take an informed decision as well as an indication of where any other information and conditions specified in regulation 42 are made available in an easily accessible manner;</p> <p>(b) it may be agreed that, by way of derogation from regulation 44, the payment service provider shall not be required to propose changes in the conditions of the framework contract in the same way as provided for in regulation 41(1);</p> <p>(c) it may be agreed that, by way of derogation from regulations 47 and 48, after the execution of a payment transaction—</p> <p>(i) the payment service provider shall provide or make available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges or, in the case of several payment transactions of the same kind made to the same</p>

		<p>payee, information on the total amount and charges for those payment transactions;</p> <p>(ii) the payment service provider shall not be required to provide or make available information referred to in subparagraph</p> <p>(i) if the payment instrument is used anonymously or if the payment service provider is not otherwise technically in a position to provide it. However, the payment service provider shall provide the payer with a possibility to verify the amount of funds stored.</p> <p>(2) The Minister may, by regulations under the principal Act–</p> <p>(a) reduce or double the amounts referred to in sub-regulation (1) for payment transactions within Gibraltar;</p> <p>(b) increase those amounts up to EUR 500 for prepaid payment instruments.</p>
CHAPTER II SINGLE PAYMENT TRANSACTIONS		
R35	Application of chapter	<p>35.(1) This Chapter applies to single payment transactions not covered by a framework contract.</p> <p>(2) When a payment order for a single payment transaction is transmitted by a payment instrument covered by a framework contract, the payment service provider shall not be obliged to provide or make available information which is already given to the payment service user on the basis of a framework contract with another payment service provider or which will be given to him according to that framework contract.</p>
R36	Prior general information	<p>36.(1) Before a payment service user is bound by any single payment service contract or offer–</p> <p>(a) the payment service provider shall make available in an easily accessible manner to the payment service user the information and conditions specified in regulation 37; and</p> <p>(b) at the payment service user's request, the payment service provider shall provide the information and conditions on paper or on another durable medium, and in both cases the information and conditions shall be provided in easily understandable words and in a clear and comprehensible form, in English or in any other language agreed between the parties.</p> <p>(2) If the single payment service contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with sub-regulation (1), the payment service provider shall fulfil its obligations under that sub-regulation immediately after the execution of the payment transaction.</p> <p>(3) The obligations under sub-regulation (1) may also be discharged by supplying a copy of the draft single payment service contract or the draft payment order including the information and conditions specified in regulation 37.</p>
R37	Information and conditions	<p>37.(1) The following information and conditions shall be provided or made available to the payment service user–</p> <p>(a) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly executed;</p> <p>(b) the maximum execution time for the payment service to be provided;</p> <p>(c) all charges payable by the payment service user to his payment service</p>

		<p>provider and, where applicable, the breakdown of the amounts of any charges;</p> <p>(d) where applicable, the actual or reference exchange rate to be applied to the payment transaction.</p> <p>(2) Where applicable, any other relevant information and conditions specified in regulation 42 shall be made available to the payment service user in an easily accessible manner.</p>
R38	Information for the payer after receipt of the payment order	<p>38. Immediately after receipt of the payment order, the payer's payment service provider shall provide or make available to the payer, in the same way as provided for in regulation 36(1), the following information–</p> <p>(a) reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee;</p> <p>(b) the amount of the payment transaction in the currency used in the payment order;</p> <p>(c) the amount of any charges for the payment transaction payable by the payer and, where applicable, a breakdown of the amounts of such charges;</p> <p>(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider or a reference thereto, when different from the rate provided in accordance with regulation 37(1)(d), and the amount of the payment transaction after that currency conversion; and</p> <p>(e) the date of receipt of the payment order.</p>
R39	Information for the payee after execution	<p>39. Immediately after the execution of the payment transaction, the payee's payment service provider shall provide or make available to the payee, in the same way as provided for in regulation 36(1), the following information–</p> <p>(a) the reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;</p> <p>(b) the amount of the payment transaction in the currency in which the funds are at the payee's disposal;</p> <p>(c) the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amount of such charges;</p> <p>(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion; and</p> <p>(e) the credit value date.</p>
CHAPTER III FRAMEWORK CONTRACTS		
R40	Application of chapter	<p>40. This Chapter applies to payment transactions covered by a framework contract.</p>
R41	Prior general information	<p>41(1) A payment service provider shall provide a payment service user with the information and conditions specified in regulation 42 as follows–</p> <p>(a) on paper or on another durable medium;</p> <p>(b) in good time before the payment service user is bound by any framework contract or offer;</p> <p>(c) in easily understandable words;</p> <p>(d) in a clear and comprehensible form; and</p> <p>(e) in English or in any other language agreed between the parties.</p> <p>(2) Where the framework contract has been concluded at the request of the payment service user using a means of distance communication which does</p>

		<p>not enable the payment service provider to comply with sub-regulation (1), the payment service provider shall fulfil its obligations under that subregulation immediately after the conclusion of the framework contract.</p> <p>(3) The obligations under sub-regulation (1) may also be discharged by supplying a copy of the draft framework contract including the information and conditions specified in regulation 42.</p>
R42	Information and conditions	<p>42. The following information and conditions shall be provided to the payment service user–</p> <p>(a) on the payment service provider–</p> <p>(i) the name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in the EEA State where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider; and</p> <p>(ii) the particulars of the relevant supervisory authorities and of the register provided for in regulation 13 or of any other relevant public register of authorisation of the payment service provider and the registration number, or equivalent means of identification in that register;</p> <p>(b) on use of the payment service–</p> <p>(i) a description of the main characteristics of the payment service to be provided;</p> <p>(ii) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly executed;</p> <p>(iii) the form of and procedure for giving consent to execute a payment transaction and withdrawal of such consent in accordance with regulations 54 and 66;</p> <p>(iv) a reference to the point in time of receipt of a payment order as defined in regulation 64 and the cut-off time, if any, established by the payment service provider;</p> <p>(v) the maximum execution time for the payment services to be provided; and</p> <p>(vi) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with regulation 55(1);</p> <p>(c) on charges, interest and exchange rates–</p> <p>(i) all charges payable by the payment service user to the payment service provider and, where applicable, the breakdown of the amounts of any charges;</p> <p>(ii) where applicable, the interest and exchange rates to be applied or, if reference interest and exchange rates are to be used, the method of calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate; and</p> <p>(iii) if agreed, the immediate application of changes in reference interest or exchange rate and information requirements related to the changes in accordance with regulation 44(2);</p> <p>(d) on communication–</p> <p>(i) where applicable, the means of communication, including the technical requirements for the payment service user's equipment, agreed between the parties for the transmission of information or notifications under these</p>

		<p>Regulations;</p> <p>(ii) the manner in and frequency with which information under these Regulations is to be provided or made available;</p> <p>(iii) language or languages in which the framework contract will be concluded and communication during this contractual relationship undertaken; and</p> <p>(iv) the payment service user's right to receive the contractual terms of the framework contract and information and conditions in accordance with regulation 43;</p> <p>(e) on safeguards and corrective measures–</p> <p>(i) where applicable, a description of steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for the purposes of regulation 56(1)(b);</p> <p>(ii) if agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with regulation 55;</p> <p>(iii) liability of the payer in accordance with regulation 61, including information on the relevant amount; (iv) how and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly executed payment transaction in accordance with regulation 58 as well as the payment service provider's liability for unauthorised payment transactions in accordance with regulation 60;</p> <p>(v) the liability of the payment service provider for the execution of payment transactions in accordance with regulation 75; and</p> <p>(vi) the conditions for refund in accordance with regulations 62 and 63;</p> <p>(f) on changes in and termination of framework contract–</p> <p>(i) if agreed, information that the payment service user will be deemed to have accepted changes in the conditions in accordance with regulation 44, unless he notifies the payment service provider that he does not accept them before the date of their proposed date of entry into force;</p> <p>(ii) the duration of the contract; and</p> <p>(iii) the right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with regulations 44(1) and 45;</p> <p>(g) on redress–</p> <p>(i) any contractual clause on the law applicable to the framework contract and/or the competent courts; and</p> <p>(ii) the out-of-court complaint and redress procedures available to the payment service user in accordance with regulations 80 to 83.</p>
R43	Accessibility of information and conditions of the framework contract	43. At any time during the contractual relationship a payment service user shall have a right to receive, on request, the contractual terms of the framework contract as well as the information and conditions specified in regulation 42 on paper or on another durable medium.
R44	Changes in conditions of the framework contract	44.(1) Any changes in the framework contract as well as the information and conditions specified in regulation 42, shall be proposed by the payment service provider in the same way as provided for in regulation 41(1) and no later than two months before their proposed date of application.

		<p>(2) Where applicable in accordance with regulation 42(f)(i), the payment service provider shall inform the payment service user that he is to be deemed to have accepted any changes proposed if he does not notify the payment service provider that he does not accept them before the proposed date of their entry into force and where this sub-regulation applies, the payment service provider shall also specify that the payment service user has the right to terminate the framework contract immediately and without charge before the date of the proposed application of the changes.</p> <p>(3) Changes in the interest or exchange rates may be applied immediately and without notice, provided that such a right is agreed upon in the framework contract and that the changes are based on the reference interest or exchange rates agreed on in accordance with regulation 42(c)(ii) and (iii).</p> <p>(4) Payment service users shall be informed of any change in the interest rate at the earliest opportunity in the same way as provided for in regulation 41(1), unless the parties have agreed on a specific frequency or manner in which the information is to be provided or made available.</p> <p>(5) Changes in interest or exchange rates which are more favourable to the payment service users, may be applied without notice.</p> <p>(6) Changes in the interest or exchange rate used in payment transactions shall be implemented and calculated in a neutral manner that does not discriminate against payment service users.</p>
R45	Termination	<p>45(1) The payment service user may terminate the framework contract at any time, unless the parties have agreed on a period of notice. Such a period may not exceed one month.</p> <p>(2) Termination of a framework contract concluded for a fixed period exceeding 12 months or for an indefinite period shall be free of charge for the payment service user after the expiry of 12 months, but in all other cases charges for the termination shall be appropriate and in line with costs.</p> <p>(3) If agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an indefinite period by giving at least two months' notice in the same way as provided for in regulation 41(1).</p> <p>(4) Charges for payment services levied on a regular basis shall be payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, they shall be reimbursed proportionally.</p> <p>(5) The provisions of this regulation are without prejudice to any statutory provision or rule of law governing the rights of parties to declare the framework contract unenforceable or void.</p> <p>(6) The Minister may, by regulations under the principal Act, provide more favourable provisions for payment service users.</p>
R46	Information before execution of individual payment transactions	<p>46. Where an individual payment transaction is made under a framework contract initiated by the payer, the payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on the maximum execution time and the charges payable by the payer and, where applicable, a breakdown of the amounts of any charges.</p>
R47	Information for the	<p>47(1) After–</p>

	payer on individual payment transactions	<p>(a) the amount of an individual payment transaction is debited from the payer's account; or</p> <p>(b) where the payer does not use a payment account, the receipt of the payment order, the payer's payment service provider shall provide the payer without undue delay in the same way as laid down in regulation 41(1) with the following information—</p> <p>(i) a reference enabling the payer to identify each payment transaction and, where appropriate, information relating to the payee;</p> <p>(ii) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;</p> <p>(iii) the amount of any charges for the payment transaction and, where applicable, a breakdown thereof, or the interest payable by the payer;</p> <p>(iv) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion; and</p> <p>(v) the debit value date or the date of receipt of the payment order.</p> <p>(2) A framework contract may include a condition that the information referred to in sub-regulation (1) is to be provided or made available periodically at least once a month and in an agreed manner which allows the payer to store and reproduce information unchanged.</p> <p>(3) However, the Minister may, by regulations under the principal Act, require payment service providers to provide information on paper once a month free of charge.</p>
R48	Information for the payee on individual payment transactions	<p>48(1) After the execution of an individual payment transaction, the payee's payment service provider shall provide the payee without undue delay in the same way as laid down in regulation 41(1) with the following information—</p> <p>(a) the reference enabling the payee to identify the payment transaction and, where appropriate, the payer, and any information transferred with the payment transaction;</p> <p>(b) the amount of the payment transaction in the currency in which the payee's payment account is credited;</p> <p>(c) the amount of any charges for the payment transaction and, where applicable, a breakdown thereof, or the interest payable by the payee;</p> <p>(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion; and</p> <p>(e) the credit value date.</p> <p>(2) A framework contract may include a condition that the information referred to in sub-regulation (1) is to be provided or made available periodically at least once a month and in an agreed manner which allows the payee to store and reproduce information unchanged.</p> <p>(3) However, the Minister may, by regulations under the principal Act, require payment service providers to provide information on paper once a month free of charge.</p>
CHAPTER IV COMMON PROVISIONS		

R49	Currency and currency conversion	49.(1) Payments shall be made in the currency agreed between the parties. (2) Where a currency conversion service is offered prior to the initiation of the payment transaction and where that currency conversion service is offered at the point of sale or by the payee, the party offering the currency conversion service to the payer shall disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction: and the payer shall agree to the currency conversion service on that basis.
R50	Information on additional charges and reductions	50.(1) Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction. (2) Where, for the use of a given payment instrument, a payment service provider or a third party requests a charge, he shall inform the payment service user thereof prior to the initiation of the payment transaction.
PART IV RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES		
CHAPTER I COMMON PROVISIONS		
R51	Scope of Part	51.(1) Where the payment service user is not a consumer, the parties may agree that regulations 52(1), 54(2)(b), 59, 61, 62, 63, 66 and 75 shall not apply in whole or in part, and the parties may also agree on a time period different from that laid down in regulation 58. (2) The Minister may, by regulations under the principal Act, provide that— (a) regulation 83 does not apply where the payment service user is not a consumer; (b) provisions in this Part are applied to micro enterprises in the same way as to consumers. (3) These Regulations shall be without prejudice to any statutory provision relating to consumer credit or the conditions for granting credit to consumers that is in conformity with European Union law.
R52	Charges applicable	52(1) The payment service provider may not charge the payment service user for fulfilment of its information obligations or corrective and preventive measures under this Part, unless otherwise specified in regulations 65(1), 66(5) and 74(2), and such charges shall be agreed between the payment service user and the payment service provider and shall be appropriate and in line with the payment service provider's actual costs. (2) Where a payment transaction does not involve any currency conversion, the payee shall pay the charges levied by his payment service provider, and the payer shall pay the charges levied by his payment service provider. (3) The payment service provider shall not prevent the payee from requesting from the payer a charge or from offering him a reduction for the use of a given payment instrument. However, the Minister may, by regulations under the principal Act, forbid or limit the right to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments.
R53	Derogation for low value payment instruments and electronic money	53(1) In the case of payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150 or store funds which do not exceed EUR 150, at any time payment service providers may agree with their payment service users that—

		<p>(a) regulations 56(1)(b), 57(1)(c) and (d) and 61(4) and (5) do not apply if the payment instrument does not allow its blocking or prevention of its further use;</p> <p>(b) regulations 59, 60, 61(1) and (2) do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;</p> <p>(c) by way of derogation from regulation 65(1), the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context;</p> <p>(d) by way of derogation from regulation 66, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee;</p> <p>(e) by way of derogation from regulations 69 and 70, other execution periods apply.</p> <p>(2) For payment transactions within Gibraltar, the Minister may, by regulations under the principal Act, reduce or double the amounts referred to in sub-regulation (1), and may increase them for prepaid payment instruments up to EUR 500.</p> <p>(3) Regulations 60 and 61 shall apply also to electronic money within the meaning of the Financial Services (Banking) Act, except where the payer's payment service provider does not have the ability to freeze the payment account or block the payment instrument, and the Minister may, by regulations under the principal Act, limit that derogation to payment accounts or payment instruments of a certain value.</p>
CHAPTER II AUTHORISATION OF PAYMENT TRANSACTIONS		
R54	Consent and withdrawal of consent	<p>54(1) A payment transaction—</p> <p>(a) shall be considered to be authorised only where the payer has given consent to execute the payment transaction;</p> <p>(b) may be authorised by the payer prior to or, if agreed between the payer and his payment service provider, after the execution of the payment transaction.</p> <p>(2) The following provisions shall apply—</p> <p>(a) consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and his payment service provider; and</p> <p>(b) in the absence of such consent, a payment transaction shall be considered to be unauthorised.</p> <p>(3) Consent—</p> <p>(a) may be withdrawn by the payer at any time, but no later than the point in time of irrevocability under regulation 66;</p> <p>(b) to execute a series of payment transactions may also be withdrawn with the effect that any future payment transaction is to be considered as unauthorised.</p> <p>(4) The procedure for giving consent shall be agreed between the payer and the payment service provider.</p>
R55	Limits of the use of the payment instrument	<p>55.(1) Where a specific payment instrument is used for the purposes of giving consent, the payer and his payment service provider may agree on spending limits for payment transactions executed through that payment instrument.</p>

		<p>(2) Where agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons related to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil his liability to pay.</p> <p>(3) In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible, before the payment instrument is blocked and at the latest immediately thereafter, unless giving such information would compromise objectively justified security reasons or is an offence.</p> <p>(4) The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.</p>
R56	Obligations of the payment service user in relation to payment instruments	<p>56.(1) The payment service user entitled to use a payment instrument shall have the following obligations–</p> <p>(a) to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument; and</p> <p>(b) to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use.</p> <p>(2) For the purposes of sub-regulation (1)(a), the payment service user shall, in particular, as soon as he receives a payment instrument, take all reasonable steps to keep its personalised security features safe.</p>
R57	Obligations of the payment service provider in relation to payment instruments	<p>57(1) The payment service provider issuing a payment instrument shall have the following obligations–</p> <p>(a) to make sure that the personalised security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in regulation 56;</p> <p>(b) to refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;</p> <p>(c) to ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to regulation 56(1)(b) or request unblocking pursuant to regulation 55(4); on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that he made such notification; and</p> <p>(d) to prevent all use of the payment instrument once notification pursuant to regulation 56(1)(b) has been made.</p> <p>(2) The payment service provider shall bear the risk of sending a payment instrument to the payer or of sending any personalised security features of it.</p>
R58	Notification of unauthorised or incorrectly executed payment transactions	<p>58. The payment service user shall obtain rectification from the payment service provider only–</p> <p>(a) where he notifies his payment service provider without undue delay on becoming aware of any unauthorised or incorrectly executed payment transactions giving rise to a claim, including that under regulation 75; and</p>

		(b) no later than 13 months after the debit date, unless, where applicable, the payment service provider has failed to provide or make available the information on that payment transaction in accordance with Part III.
R59	Evidence on authentication and execution of payment transactions	59(1) Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency. (2) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under regulation 56.
R60	Payment service provider's liability for unauthorised payment transactions	60(1) Without prejudice to regulation 58, in the case of an unauthorised payment transaction, the payer's payment service provider shall— (a) refund to the payer immediately the amount of the unauthorised payment transaction; and (b) where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. (2) Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and his payment service provider
R61	Payer's liability for unauthorised payment transactions	61(1) By way of derogation from regulation 60, the payer shall bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment instrument or, if the payer has failed to keep the personalised security features safe, from the misappropriation of a payment instrument. (2) The payer shall bear all the losses relating to any unauthorised payment transactions if he incurred them by acting fraudulently or by failing to fulfil one or more of his obligations under regulation 56 with intent or gross negligence; and in such cases, the maximum amount referred to in sub-regulation (1) shall not apply. (3) In cases where the payer has not acted fraudulently or with intent failed to fulfil his obligations under regulation 56, the Minister may, by regulations under the principal Act, reduce the liability referred to in subregulations (1) and (2), taking into account, in particular, the nature of the personalised security features of the payment instrument and the circumstances under which it was lost, stolen or misappropriated. (4) The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with regulation 56(1)(b), except where he has acted fraudulently. (5) Where the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under regulation 57(1)(c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument,

		except where he has acted fraudulently.
R62	Refunds for payment transactions initiated by or through a payee	<p>62(1) A payer shall be entitled to a refund, consisting of the full amount of the executed payment transaction, from his payment service provider of an authorised payment transaction initiated by or through a payee which has already been executed, where the following conditions are met–</p> <p>(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made; and</p> <p>(b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account his previous spending pattern, the conditions in his framework contract and relevant circumstances of the case; and–</p> <p>(i) at the payment service provider’s request, the payer shall provide factual elements relating to such conditions;</p> <p>(ii) for direct debits the payer and his payment service provider may agree in the framework contract that the payer is entitled to a refund from his payment service provider even though the conditions for refund in sub-paragraphs (a) and (b) above are not met.</p> <p>(2) For the purposes of sub-regulation (1)(b), the payer may not rely on currency exchange reasons if the reference exchange rate agreed with his payment service provider in accordance with regulations 37(1)(d) and 42(3)(b) was applied.</p> <p>(3) It may be agreed in the framework contract between the payer and the payment service provider that the payer has no right to a refund–</p> <p>(a) where he has given his consent to execute the payment transaction directly to his payment service provider; and</p> <p>(b) where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least four weeks before the due date by the payment service provider or by the payee.</p>
R63	Requests for refunds for payment transactions initiated by or through a payee	<p>63(1) The payer may request the refund referred to in regulation 62 of an authorised payment transaction initiated by or through a payee for a period of eight weeks from the date on which the funds were debited.</p> <p>(2) Within ten business days of receiving such a request for a refund, the payment service provider shall either–</p> <p>(a) refund the full amount of the payment transaction; or</p> <p>(b) provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter in accordance with regulations 80 to 83 if he does not accept the justification provided.</p> <p>(3) The payment service provider’s right under sub-regulation (2) to refuse the refund shall not apply in the case set out in regulation 62(1)(ii).</p>
CHAPTER III EXECUTION OF PAYMENT TRANSACTIONS		
R64	Receipt of payment orders	<p>64.(1) The point in time of receipt of a payment order shall be–</p> <p>(a) the time when the payment order transmitted directly by the payer or indirectly by or through a payee is received by the payer’s payment service provider; and</p> <p>(b) where the point in time of receipt is not on a business day for the payer’s payment service provider, the payment order shall be deemed to have been received on the following business day, and the payment service provider may</p>

		<p>establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.</p> <p>(2) Where the payment service user initiating a payment order and his payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has set funds at his payment service provider's disposal, the point in time of receipt for the purposes of regulation 69 shall be deemed to be the agreed day; and where the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.</p>
R65	Refusal of payment orders	<p>65.(1) The following provisions shall apply–</p> <p>(a) where the payment service provider refuses to execute a payment order, the refusal and, if possible, the reasons for it and the procedure for correcting any factual mistakes that led to the refusal shall be notified to the payment service user, unless it is an offence to notify such information;</p> <p>(b) the payment service provider shall provide or make available the notification in an agreed manner at the earliest opportunity, and in any case, within the periods specified in regulation 69; and</p> <p>(c) the framework contract may include a condition that the payment service provider may charge for such a notification if the refusal is objectively justified.</p> <p>(2) Where all the conditions set out in the payer's framework contract are met, the payer's payment service provider shall not refuse to execute an authorised payment order irrespective of whether the payment order is initiated by a payer or by or through a payee, unless it is an offence.</p> <p>(3) For the purposes of regulations 69 and 75 a payment order of which execution has been refused shall be deemed not to have been received.</p>
R66	Irrevocability of a payment order	<p>66(1) The payment service user may not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in this regulation.</p> <p>(2) Where the payment transaction is initiated by or through the payee, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee.</p> <p>(3) In the case of a direct debit, and without prejudice to refund rights, the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds.</p> <p>(4) In the case referred to in regulation 64(2) the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.</p> <p>(5) After the time limits specified in sub-regulations (1) to (4)–</p> <p>(a) the payment order may be revoked only if agreed between the payment service user and his payment service provider; and</p> <p>(b) for the purposes of sub-regulations (2) and (3), the payee's agreement shall also be required.</p> <p>(6) If agreed in the framework contract, the payment service provider may charge for revocation.</p>
R67	Amounts	<p>67.(1) Subject to sub-regulation (2), the payment service provider of the payer,</p>

	transferred and amounts received	<p>the payment service provider of the payee and any intermediaries of the payment service providers shall transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.</p> <p>(2) The payee and his payment service provider may agree that the payment service provider deduct its charges from the amount transferred before crediting it to the payee, and in such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.</p> <p>(3) Where any charges other than those referred to in sub-regulation (2) are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. In cases where the payment transaction is initiated by or through the payee, his payment service provider shall ensure that the full amount of the payment transaction is received by the payee.</p>
R68	Scope of this regulation and regulations 69 to 73	<p>68(1) This regulation and regulations 69 to 73 apply to–</p> <p>(a) payment transactions in Euro;</p> <p>(b) payment transactions in Sterling or Gibraltar Pounds within Gibraltar or between Gibraltar and the United Kingdom in Sterling; and</p> <p>(c) payment transactions involving only one currency conversion between the Euro and Sterling, provided that the required currency conversion is carried out in Gibraltar and, in the case of cross-border payment transactions, the cross-border transfer takes place in Euro.</p> <p>(2) The following provisions shall apply–</p> <p>(a) this regulation and regulations 69 to 73 shall apply to other payment transactions, unless otherwise agreed between the payment service user and his payment service provider, with the exception of regulation 73, which is not at the disposal of the parties;</p> <p>(b) when the payment service user and his payment service provider agree on a longer period than any of those laid down in regulation 69, for intra-European Union payment transactions such period shall not exceed 4 business days following the point in time of receipt in accordance with regulation 64.</p>
R69	Payment transactions to a payment account	<p>69(1) The payer's payment service provider shall ensure that, after the point in time of receipt in accordance with regulation 64, the amount of the payment transaction shall be credited to the payee's payment service provider's account at the latest by the end of the next business day. However, until 1 January 2012, a payer and his payment service provider may agree on a period no longer than three business days. These periods may be extended by a further business day for paper-initiated payment transactions.</p> <p>(2) The payment service provider of the payee shall value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with regulation 73.</p> <p>(3) The payee's payment service provider shall transmit a payment order initiated by or through the payee to the payer's payment service provider within the time limits agreed between the payee and his payment service provider, enabling settlement, as far as direct debit is concerned, on the agreed due date.</p>

R70	Absence of payee's payment account with the payment service provider	70. Where the payee does not have a payment account with the payment service provider, the funds shall be made available to the payee by the payment service provider who receives the funds for the payee within the period specified in regulation 69.
R71	Cash placed on a payment account	71. Where— (a) a consumer places cash on a payment account with a payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after the point of time of the receipt of the funds; (b) the payment service user is not a consumer, the amount shall be made available and value dated at the latest on the next business day after the receipt of the funds.
R72	Payment transactions within Gibraltar	72. For payment transactions within Gibraltar, the Minister may, by regulations under the principal Act, provide for shorter maximum execution times than those provided for in regulations 68 to 71 and 73.
R73	Value date and availability of funds	73(1) The following provisions shall apply— (a) the credit value date for the payee's payment account shall be no later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account; and (b) the payment service provider of the payee shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account. (2) The debit value date for the payer's payment account shall be no earlier than the point in time at which the amount of the payment transaction is debited to that payment account.
R74	Incorrect unique identifiers	74(1) Where a payment order is executed in accordance with the unique identifier, it shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier. (2) The following provisions shall apply— (a) where the unique identifier provided by the payment service user is incorrect, the payment service provider shall not be liable under regulation 75 for non-execution or defective execution of the payment transaction; (b) the payer's payment service provider shall make reasonable efforts to recover the funds involved in the payment transaction; and (c) where agreed in the framework contract, the payment service provider may charge the payment service user for recovery. (3) Where the payment service user provides information additional to that specified in regulations 37(1)(a) or 42(2)(b), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.
R75	Non-execution or defective execution	75(1) Where— (a) a payment order is initiated by the payer, his payment service provider shall, without prejudice to regulations 58, 74(2) and (3) and 78, be liable to the payer for correct execution of the payment transaction, unless he can prove to the payer and, where relevant, to the payee's payment service provider, that the payee's payment service provider

		<p>received the amount of the payment transaction in accordance with regulation 69(1), in which case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction;</p> <p>(b) he payer's payment service provider is liable under paragraph (a), he shall without undue delay refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place;</p> <p>(c) the payee's payment service provider is liable under paragraph (a), he shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account, and in the case of a non-executed or defectively executed payment transaction where the payment order is initiated by the payer, his payment service provider shall, regardless of liability under this sub-regulation, on request, make immediate efforts to trace the payment transaction and notify the payer of the outcome.</p> <p>(2) The following provisions apply–</p> <p>(a) where a payment order is initiated by or through the payee, his payment service provider shall, without prejudice to regulations 58, 74(2) and (3) and 78, be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with regulation 69(3), and where the payee's payment service provider is liable under this paragraph, he shall immediately re-transmit the payment order in question to the payment service provider of the payer;</p> <p>(b) the payment service provider of the payee shall, without prejudice to regulations 58, 74(2) and (3) and 78, in addition be liable to the payee for handling the payment transaction in accordance with its obligations under regulation 73, and where the payee's payment service provider is liable under this paragraph, he shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account;</p> <p>(c) in the case of a non-executed or defectively executed payment transaction for which the payee's payment service provider is not liable under paragraphs (a) and (b), the payer's payment service provider shall be liable to the payer, and where the payer's payment service provider is so liable he shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place; and</p> <p>(d) in the case of a non-executed or defectively executed payment transaction where the payment order is initiated by or through the payee, his payment service provider shall, regardless of liability under this sub-regulation, on request, make immediate efforts to trace the payment transaction and notify the payee of the outcome.</p> <p>(3) Payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution</p>
--	--	---

		or defective execution of the payment transaction.
R76	Additional financial compensation	76. Any financial compensation additional to that provided for under regulations 74 to 75 and 77 to 78, may be determined in accordance with the law applicable to the contract concluded between the payment service user and his payment service provider.
R77	Right of recourse	77.(1) Where the liability of a payment service provider under regulation 75 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under regulation 75. (2) Further financial compensation may be determined in accordance with agreements between payment service providers and/or intermediaries and the law applicable to the agreement concluded between them.
R78	No liability	78. Liability under this Chapter and Chapter II shall not apply in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other statutory obligations.
CHAPTER IV DATA PROTECTION		
R79	Data protection	79(1) The Commissioner shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. (2) The processing of personal data under sub-regulation (1) shall be carried out in accordance with the Data Protection Act 2004. (3) In sub-regulation (1), "Commissioner" shall be interpreted in accordance with section 2 of the Data Protection Act 2004.
CHAPTER V OUT-OF-COURT COMPLAINT AND REDRESS PROCEDURES FOR THE SETTLEMENT OF DISPUTES		
R80	Complaints	80(1) Payment service users and other interested parties, including consumer associations, may submit complaints to the competent authority with regard to payment service providers' alleged infringements of the provisions of these Regulations. (2) Where appropriate and without prejudice to the right to bring proceedings before the Supreme Court, the reply from the competent authority shall inform the complainant of the existence of the out-of-court complaint and redress procedures set up in accordance with regulation 83.
R81	Penalties	81(1) A payment service user or provider that is responsible for any act or omission contrary to the provisions of these Regulations commits an offence. (2) A payment service user or provider found guilty of an offence contrary to sub-regulation (1) is liable on summary conviction to a fine not exceeding level 5 on the standard scale.
R82	Competent authorities for complaints	82(1) Where there has been an infringement or suspected infringement of the provisions of Parts III and IV by a payment service provider where Gibraltar is the host EEA State, the competent authority responsible for hearing complaints and imposing penalties shall be that of the home EEA State, except for agents and branches operating in Gibraltar under the right of establishment in respect of whom the competent authority shall be that described in

		<p>regulation 2.</p> <p>(2) Where there has been an infringement or suspected infringement of the provisions of Parts III and IV by a payment service provider where Gibraltar is the home EEA State, the competent authority responsible for hearing complaints and imposing penalties shall be that described in regulation 2, except for agents and branches operating elsewhere in the EEA under the right of establishment in respect of whom the competent authorities shall be those of the host EEA State.</p>
R83	Out-of-court redress	<p>83(1) The provisions of the <u>Arbitration Act shall apply for the settlement of disputes between payment service users and their payment service providers concerning rights and obligations arising under these Regulations</u> as if there were an Arbitration Agreement between them providing for the reference of disputes between them to an official referee for all the purposes of section 7 of the Arbitration Act.</p> <p>(2) In the case of <u>cross-border disputes</u>, the competent authority shall facilitate and encourage the cooperation of the bodies or persons actively involved in resolving disputes referred to in sub-regulation (1).</p>
PART V: FINAL PROVISIONS		
R84	Derogations from Act	<p>Any attempt by a payment service providers to derogate, to the detriment of payment service users, from the provisions of these Regulations shall be unenforceable save where explicitly provided for in these Regulations, but payment service providers may decide to grant more favourable terms to payment service users.</p>
R85	Transitional provision	<p>85(1) Legal persons who, before 25 December 2007, have lawfully commenced the activities of payment institutions, within the meaning of these Regulations, may continue to do so until 30 April 2011 without authorisation under regulation 10; but any such persons who have not been granted authorisation within this periods hall, pursuant to regulation 29, be prohibited from providing payment services as from that date.</p> <p>(2) Notwithstanding sub-regulation (1) and subject to sub-regulation (3), an exemption to the authorisation requirement under regulation 10 shall be granted by the competent authority to–</p> <p>(a) financial institutions that have commenced money transmission services under the Financial Services (Banking) Act;</p> <p>(b) since 25 December 2007, such services have been effectively included in the consolidated supervision of the parent undertaking, or of each of the parent undertakings of that financial institution in accordance with the provisions of the Financial Services (Banking) Act; and</p> <p>(c) the consolidated supervision referred to in paragraph (b), focused in particular on the minimum own funds requirements set out in the Financial Services(Banking) Act for the control of large exposures and for the purposes of the limitation of holdings provided for in that Act.</p> <p>(3) The competent authority shall have notified the competent authorities of the home EEA State of these activities by 25 December 2007. This notification shall have included the information demonstrating that they have complied with regulation 5(a), (d), (g) to (i), (k) and (l) of these Regulations. Where the competent authorities of the home EEA State are satisfied that those</p>

		<p>requirements are complied with, the financial institutions concerned shall be registered in accordance with regulation 13 of these Regulations, and the Minister may, by regulations under the principal Act, allow the competent authority to exempt those financial institutions from the requirements under regulation 5.</p> <p>(4) The Minister may, by regulations under the principal Act, provide that legal persons referred to in sub-regulation (1) shall be automatically granted authorisation and entered into the register provided for in regulation 13 if the competent authority already has evidence that the requirements laid down in regulations 5 and 10 are complied with, and the competent authority shall inform the entities concerned before the authorisation is granted.</p> <p>(5) The competent authority may allow persons who have lawfully commenced the activities of payment institutions within the meaning of these Regulations before 25 December 2007 and who are eligible for waiver under regulation 26 to continue those activities within Gibraltar for a transitional period not longer than 3 years without being waived in accordance with regulation 26 and entered into the register provided for in regulation 13. It shall be an offence for any such persons who are not waived within the said period of 3 years to provide payment services.</p>
R86	Schedule	As below.

SCHEDULE: PAYMENT SERVICES

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.
2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.
3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider–
 - (a) execution of direct debits, including one-off direct debits;
 - (b) execution of payment transactions through a payment card or a similar device;
 - (c) execution of credit transfers, including standing orders.
4. Execution of payment transactions where the funds are covered by a credit line for a payment service user–
 - (a) execution of direct debits, including one-off direct debits;
 - (b) execution of payment transactions through a payment card or a similar device;
 - (c) execution of credit transfers, including standing orders.
5. Issuing and/or acquiring of payment instruments.
6. Money remittance.
7. Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

INDIVIDUALS INTERVIEWED

ANGOLA¹⁰⁴⁹

Banco Nacional de Angola	Joao Romao Coje
Banco Nacional de Angola	Joaquim Augusto Canico
Banco Nacional de Angola	Luis Filipe Gomes Manuel
Banco Nacional de Angola	Victor Ferreira Rodrigues
Banco Nacional de Angola	Júlia Ointo Jerónimo
Banco Nacional de Angola	Clara Santiago
Banco Nacional de Angola	Teresa de Fatima
Banking Association	Katila Santos
FIU	Francisca de Brito
EMIS	Solange Costa
EMIS	Adilson Dange
Banco Angolano de Investimentos	Carla Pataca
Banco Angolano de Investimentos	Alfredo Oliveira
Banco Angolano de Investimentos	Henrique dos Santos
Banco Angolano de Investimentos	Manuel Cardoso

BOTSWANA¹⁰⁵⁰

Bank of Botswana NPS	Ewetse Rakhudu
Bank of Botswana NPS	Morgan Setlhako
Bank of Botswana NPS	Maria Radibe
Bank of Botswana NPS	Lebogang Motumise
Bank of Botswana Information Technology Department	Julius Ghanie
SADC FIP Liaison	Chepete Chepete
Bankers Association of Botswana (BAB)	Oabile Mabusa
Bank of Botswana Banking Supervision	Andrew Motsumi
Financial Intelligence Agency	Jackson Madzima
SmartSwitch	Kevin Duke
SmartSwitch	Celia Ajuba
Standard Chartered Bank of Botswana Ltd	Ediretse Ramahobo
Electronic Clearing House (ECH) Manager	Julia Kgoadi
Botswana Stock Exchange (BSE)	Mr H Mendis
Botswana Stock Exchange (BSE) (CSD Manager)	Masego Pheto
Non-Bank Financial Institutions Regulatory Authority (NBFIRA)	Oaitse Ramasedi and colleagues
Ministry of Transport and Communications	Mabua Mabua

¹⁰⁴⁹ Dates of in-country interviews: 25 June 2013 – 27 June 2013.

¹⁰⁵⁰ Dates of in-country interviews: 11 February 2013 – 12 February 2013.

DRC¹⁰⁵¹

Banque Centrale du Congo NPS	Kapinga Tsim Ngele
Banque Centrale du Congo NPS	Mukengeshay Katalay
Banque Centrale du Congo	Oliver Nzanza Lukau
Banque Centrale du Congo Direction de la Surveillance des Intermédiaires Financiers	Jean Marcel Kalubi Kayembe
Banque Centrale du Congo Direction Générale de la Politique Monétaire et des Opérations Bancaires	Jean Louis Kayembe
	Michel-Edouard Wembandju
Banque Centrale du Congo	Odimba
Ministry of Finance National Consultant FIP for SADC	Pascal Didier Muderwa Marandura
Ministry of Finance	Kally Muzuri Nyembo Mwana
	Katualla Kaba Kashala and colleagues
CENAREF (FIU)	Patrice Buabua Kadima
FIBank	Eric Mboma
Standard Bank	Celestin Makangu and colleagues
Bankers Association	Christian Kamanzi Muhindo
Rawbank	

LESOTHO¹⁰⁵²

Central Bank of Lesotho NPS	Seabata Ntelo
Central Bank of Lesotho NPS	Malineo Motebang
Central Bank of Lesotho NPS	Mankaba Thabane
Central Bank of Lesotho (Legal Services)	Nthati Mokitimi
Central Bank of Lesotho / FIU	Palesa Khabele
Standard Bank Lesotho / Bankers Association	Mohau Masia
Ministry of Finance (Legal)	Motale Ts'eole
Payments Advisor Central Bank of Lesotho	Grey Nkungula

MALAWI¹⁰⁵³

Reserve Bank of Malawi NPS	Fraser Mdwazika
Reserve Bank of Malawi NPS	Osky Sichinga
Reserve Bank of Malawi Legal	George Chioza
Reserve Bank of Malawi NPS	Grace Mbera
Reserve Bank of Malawi AML/CFT Bank Supervision	Thelma Tiyanjane Saiwa
Reserve Bank of Malawi Bank Supervision	William Masamba
Reserve Bank of Malawi Bank Supervision	Hains Munthali
Reserve Bank of Malawi Bank Supervision	Suzgo Muntahli
Reserve Bank of Malawi Bank Supervision	Sam Chilunga

¹⁰⁵¹ Dates of in-country interviews: 3 July 2013 – 5 July 2013.

¹⁰⁵² Dates of in-country interviews: 25 February 2013 – 27 February 2013.

¹⁰⁵³ Dates of in-country interviews: 27 May 2013 – 30 May 2013.

Reserve Bank of Malawi Bank Supervision
Pensions and Insurance
FIU
FIU
Stock Exchange
Ecobank (Legal)

National Bank of Malawi (Legal Counsel)
National Bank of Malawi (Legal Counsel)
Malswitch
Malswitch
Malawi Bankers Association - National Bank of Malawi
Malawi Bankers Association - Indebank
Malawi Bankers Association - Malawi Savings Bank
Malawi Bankers Association - First Merchant Bank
Malawi Bankers Association -First Discount House
Malawi Bankers Association - Ned Bank
Priscilla Mchenga-Vice Chair
Evans Chitsanthi
Mercy Mthimbwa
Neema Kasiya
Annastasia Nkhata
Oswell Sulapa
Fredrick Thengeza
Lyness Nkungula
Joy Mawindo
Mbongeni Chizonda
Ruth Ntupanyama
Austin Mtonga
Patrick Ibrhim

Yananga Phiri
Paul Nyirenda
Masautso Ebere
Anita Mankhambo
Symon Msefula
Luke Katayika
Gilbert Konsekonse
Chibesakunda
Zunzo Mitole
Gladson Kuyeri
Francis Bisika
Brian Boby
Emily Makuta
Faniel Kumdana
Edward Msukwa
James Chikoti
Julius Nyaka
NBS Bank
FMB
STD Bank
Ecobank
ICB
Indebank
RBM
BAM
MALSWITCH
BAM
STD Bank
NBS Bank
RBM

MAURITIUS¹⁰⁵⁴

Bank of Mauritius Payment Systems & MCIB
Bank of Mauritius Legal
Central Depository & Settlement Co. Ltd
Financial Intelligence Unit
Mauritius Bankers Association Limited
MCB Cards
MCB Cards
MCB Swift
MCB Operations

Dhanesswurnath Vikash
Thakoor
Rajshri Jutton Gopy
Vipin Mahabirsingh
Dev Bikoo
Aisha Timol
Binesh Mangar
Patrick Hope
Kumar Beezlo
Peter Bakewell Haddon

¹⁰⁵⁴ Dates of in-country interviews: 20 May 2013 – 22 May 2013.

MCB Operations
 MCB Finance and Administration
 Stock Exchange of Mauritius Ltd
 State Bank of Mauritius
 State Bank of Mauritius
 AAMIL

Maryline Moteea
 Bernard Jackson
 Sunil Benimadhu
 Balkrishna Jhurry
 Anil Gujjalu
 Rama Appadoo

MOZAMBIQUE¹⁰⁵⁵

Banco de Moçambique NPS
 Banco de Moçambique NPS
 Banco de Moçambique Legal
 Banco de Moçambique NPS
 Banco de Moçambique Legal
 Banco de Moçambique NPS
 Banco de Moçambique Legal
 Banco de Moçambique Bank Supervision
 Interbancos

Henrique Matsinhe
 Gabriel Domingos
 Edson Laice
 Aurora Da Glória V. Bila
 Rui Baessa Pinto
 Carlota Nhampule
 Mussa Mussa
 Juvêncio Nhaúle
 Carlos Street Lemos

NAMIBIA¹⁰⁵⁶

Bank of Namibia Payment and Settlement System Department
 Bank of Namibia Payment and Settlement System Department
 Bank of Namibia Payment and Settlement System Department
 Bank of Namibia Payment and Settlement System Department
 Bank of Namibia Head of Legal Services and Contract Management
 Bank of Namibia (IT Department)
 Bank of Namibia FIC
 Bank of Namibia FIC
 Bank of Namibia FIC
 Bank of Namibia FIC
 Bank of Namibia FIC
 Bank of Namibia Banking Services
 Bank of Namibia Currency and Banking Services Department
 Bank of Namibia Currency and Banking Services Department
 Bank of Namibia Currency and Banking Services Department
 Bank of Namibia Currency and Banking Services Department
 Bank of Namibia Bank Supervision
 Bank of Namibia Bank Supervision (Banking Groups)
 Bank of Namibia Financial Markets
 Bank of Namibia Financial Markets
 Bank of Namibia Financial Markets

Brian Gei-Khoibeb
 Sergio de Sousa
 Barbara Gowaseb
 Moody Tembo
 Tulonga Nakamhela
 Justice Kapitango
 Leonie Dunn
 Zenobia Barry
 Erika Shikusinde
 Issy Tjihoreko
 Nicky Mupetami
 Barbie Botma
 John Amakali
 Sencia Rukata
 Cillie Isaacs
 Lorraine Msomi
 Romeo Nel
 Njekwa Mwamba-Haufiku
 Titus Ndove
 Maano Nepembe
 Sam Shivute

¹⁰⁵⁵ Dates of in-country interviews: 1 June 2013 – 5 June 2013.

¹⁰⁵⁶ Dates of in-country interviews: 4 February 2013 – 6 February 2013.

Payments Association of Namibia
 Payments Association of Namibia
 Payments Association of Namibia
 Namibian Stock Exchange
 Bank Windhoek
 First National Bank
 Namibian Stock Exchange
 Namswitch/Namclear

Annette Rathenam
 Mberipura Hifitikeko
 Lydia Iiyambo
 Tiaan Bazuin
 Chris Diemer
 Francois Botha
 John D. Mandy
 Fabian Tait

SEYCHELLES¹⁰⁵⁷

Central Bank of Seychelles Governor
 Central Bank of Seychelles National Payment Systems Unit
 Central Bank of Seychelles National Payment Systems Unit
 Central Bank of Seychelles National Payment Systems Unit
 Central Bank of Seychelles
 Central Bank of Seychelles Banking Services
 Central Bank of Seychelles -Financial Market Division
 Central Bank of Seychelles Policy Unit
 Central Bank of Seychelles FS Analyst
 Central Bank of Seychelles Legal
 Financial Intelligence Unit
 Financial Intelligence Unit
 Seychelles Savings Bank /Bankers Association
 Mauritius Commercial Bank (Seychelles)
 Mauritius Commercial Bank (Seychelles) - Operations
 Seychelles Payment Services
 Ministry of Finance
 Ministry of Finance
 Ministry of Finance / Treasury
 University of Seychelles
 Bank of Baroda
 Bank of Baroda

Caroline Abel
 Patricia Padayachy
 Terry Adrienne
 Nadia Gabriel
 Jenifer Sullivan
 Mike Tirant
 Moyra Alexis
 Joan Lespoir
 Nicolas Cepoute
 Shannon Jolicoeur
 Phillip Moustache
 Jeannieve Volcere
 Micheal Benstrong
 Bernard Jackson
 Régis Bistoquet
 Hala Abu Hantash
 Patrick Payet
 Damien Thesee
 Mrs. Gretel Quatre
 Shella Mohideen
 Mr Alok Kumar
 Mr. L Shadeo

SOUTH AFRICA

South African Reserve Bank, Bank Supervision (AML/CFT)
 South African Reserve Bank, Bank Supervision (AML/CFT)
 South African Reserve Bank, NPSD
 South African Reserve Bank, NPSD
 South African Reserve Bank, NPSD
 South African Reserve Bank, NPSD
 South African Reserve Bank, (Legal)

Denzel Bostander
 Stephen Mkwanzazi
 Edward Leach
 Magedi-Titus Thokwane
 Tim Masela
 Anrich Daseman
 Jana van Staden

¹⁰⁵⁷ Dates of in-country interviews: 10 June 2013 – 13 June 2013.

South African Reserve Bank, (Legal)
 FIC
 FIC
 PASA
 PASA
 VISA
 VISA
 VISA

Bernard Khoza
 Prenisha Jagganath
 Pieter Smit
 Walter Volker
 Pierre Coetzee
 Layla Moosa
 Daniel Ngwepe
 Lenny Kunga

SWAZILAND¹⁰⁵⁸

Central Bank of Swaziland NPS
 Central Bank of Swaziland NPS
 Central Bank of Swaziland NPS
 Central Bank of Swaziland
 Central Bank of Swaziland
 Central Bank of Swaziland Bank Supervision (Examiner)
 Central Bank of Swaziland Exchange Control
 Central Bank of Swaziland (AML Officer)
 Swazibank
 Swazibank
 Swazibank
 Stock Exchange

Mandla Dlamini
 Lindiwe Mango
 Fikile Shongwe
 Refiloe Mamogobo
 Mazwi I. Simelane
 Thulani Mnisi
 Mduduzi Tustin Mtsetfwa
 Bheki Khumalo
 Sifiso C. Mdluli
 Babhekile Dlamini
 Lindiwe Pinky Mango
 Peace Mabuza

ZAMBIA¹⁰⁵⁹

Bank of Zambia Payment Systems
 Bank of Zambia Payment Systems
 Bank of Zambia Payment Systems
 Bank of Zambia Payment Systems
 Bank of Zambia Payment Systems
 Bank of Zambia Payment Systems
 Ecobank / Zambian Bankers Association
 Investrust Bank Plc
 FIA
 FIA
 FIA
 Ministry of Transport, Works Supply and Communications / ZICTA
 Ministry of Transport, Works Supply and Communications / ZICTA
 Zambia Electronic Clearing House Ltd
 Zamlink / eSwitch Zambia Ltd t/a

Lazarous Kamanga
 Mirriam Kamuhuza
 Maria Katepa
 Angela Nachivula
 Mwelwa Mwaba
 Cosmas Soko
 Jinga Kapihya
 Pinzya Butambo Sikasula
 Isaac Chilanga
 Miyanda Siamoongwa
 Imattaa Mubialelwa
 Benaiah Mpange
 Mupenda
 Thomas Malama
 Christopher Mwanza
 Eddie Muyeba

¹⁰⁵⁸ Dates of in-country interviews: 28 February 2013 – 1 March 2013.

¹⁰⁵⁹ Dates of in-country interviews: 13 February 2013 – 15 February 2013.

Zamlink / eSwitch Zambia Ltd t/a
 Zamlink / eSwitch Zambia Ltd t/a
 LUSE
 LUSE
 LUSE
 Securities and Exchange Commission
 Payments Association of Zambia
 Calltrol Zambia

James Jumbe
 Victoria Chilufya
 Joel Mbulo
 Priscilla Sampa
 Sondo Musona
 Constantine Hara
 Iris Nwanza
 Justin Birch

ZIMBABWE¹⁰⁶⁰

Reserve Bank of Zimbabwe National Payment Systems
 Reserve Bank of Zimbabwe National Payment Systems
 Reserve Bank of Zimbabwe National Payment Systems
 Reserve Bank of Zimbabwe National Payment Systems
 Reserve Bank of Zimbabwe Bank Supervision
 Reserve Bank of Zimbabwe Bank Supervision
 Reserve Bank of Zimbabwe Bank Supervision
 BUP & FI (AML)
 BUP & FI (AML)
 BUP & FI (AML)
 BUP & FI (AML)
 BUP & FI (AML)
 Securities Commission of Zimbabwe

 Securities Commission of Zimbabwe
 ZimSwitch Shared Services
 ZimSwitch Shared Services
 ZimSwitch Shared Services
 ZimSwitch Shared Services
 CABS
 CABS
 CABS
 CABS
 CABS

Amon Chitsva
 Josephat Mutepfa
 Douglas Muranda
 Julia Njobo
 Cosmas Kanhai
 Norman Mataruka
 Norah Mukura
 Oliver Chiperesa
 Clara Hwata
 Wonder Kapofu
 Tongesai Murape
 Kenneth Ngwarai
 Norman Maferefa
 Mr. Tafadzwa
 Chinhamo
 Adam Roscoe
 Derek Vincent
 Tinashe Matombo
 Cyril Nyatsanza
 Frances Pickering
 Kevin Terry
 Emily Crookes
 Farirayi Machawira
 Josephine Javangwe

¹⁰⁶⁰ Dates of in-country interviews: 20 February 2013 – 22 February 2013.

ACRONYMNS

ABANC	Associacao Angolana De Bancos
ACH	Automated Clearing House
AES	Advanced Encryption Standard
ANG	Angola
EFT	Electronic Funds Transfer
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
APGM	Asia/Pacific Group on Money Laundering
ATM	Automated Teller Machine
ATS	Automated Transfer System
BAM	Bankers Association of Malawi
BBAN	Base Bank Account Number
BIC	Business Identifier Codes
BIS	Bank for International Settlements
BISS	Botswana Interbank Settlement System
BSD	Banking Supervision Department
BWA	Botswana
CBSITS	Central Bank of Seychelles Immediate Transfer Service
CCSNP	National Payment System Coordinating Committee (English Translation)
CCBG	Committee of Central Bank Governors
CCP	Central Counterparties
CDD	Customer Due Diligence
CENAREF	<i>Cellule Nationale des Renseignements Financiers</i> (DRC)
CFT	Countering the Financing of Terrorism
CITS	Cheque Imaging and Truncation System
CLS	Continuous Linked Settlement
CMA	Common Monetary Area
COMESA	Common Market for Eastern and Southern Africa
COSSE	Committee of SADC Stock Exchanges
CPS	Cheque Processing System
CPSIPS	Core Principles for Systemically Important Payment Systems
CPSS	Committee on Payment and Settlement Systems
CSD	Central Securities Depositories
CSDB	Central Securities Depository Botswana
DECH	Dar es Salaam Electronic Clearing House
DES	Triple Data Encryption Standard or
DCEC	Directorate of Corruption and Economic Crime
DDACC	Direct Debit and Credit Clearing (Zambia)
DNFBPs	Designated Non-Financial Businesses and Professions
DRC	Democratic Republic of the Congo
DvD	Delivery versus Delivery
DvP	Delivery versus Payment
EAC	East African Community

EC	European Commission
ECC	Electronic Cheque Clearing
ECH	Electronic Clearing House
ECCH	Electronic Cheque Clearing House
ECOWAS	Economic Community Of West African States
EDI	Electronic Data Interchange
EDO	Early Debit Order
EFS	Electronic Financial Surveillance
EFT	Electronic Funds Transfer
EMU	Economic and Monetary Union
EPC	European Payments Council
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
ESMA	European Securities and Markets Authority
EUR	Euro
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
FIC	Financial Intelligence Centre
FIP	Protocol on Finance and Investment (SADC)
FIU	Financial Intelligence Unit
FMI	Financial Markets Infrastructures
FSB	Financial Services Board
FSC	Financial Services Commission
FSRBs	FATF-Style Regional Bodies
FSTAP	Financial Sector Technical Assistance Program
GPRS	General Packet Radio Service
HSM	Hardware Security Module
IBAN	International Bank Account Numbers
ICM	Integrated Committee of Ministers
ICTA	Information and Communication Technologies Authority
IDS	Intrusion Detection systems
ILF	Intraday Liquidity Facility
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
IVR	Interactive Voice Response
KYC	Know Your Customer
LRR	Liquidity Reserve Requirement
LSO	Lesotho
LSW	Lesotho Wire
LUSE	Lusaka Stock Exchange
MACSS	Mauritius Automated Clearing and Settlement System
MCX	Multicaixa Subsystem (Angola)
MITASS	Malawi Interbank Transfers and Settlement System
MOU	Memorandum of Understanding
MRA	Master Repurchase Agreement
MTR	Metical em Tempo Real (Mozambique)

MU	Mauritius
MVTS	Money or Value Transfer Services
MW	Malawi
MZ	Mozambique
NA	Namibia
NAEDO	Non-Authenticated Early Debit Orders
NBFI	Non-bank Financial Institution
NISS	Namibia Inter-bank Settlement System
NLP	New Legal Framework for Payments
NPPS	New Payment Products and Services
NPS	National Payment System
NPSAB	National Payment System Advisory Body (South Africa)
NPSD	National Payment System Department
NPSSB	National Payment System Strategy Body (South Africa)
OHADA	Organisation pour l'Harmonisation en Afrique du Droit des Affaires
OPDSC	Organ on Politics, Defense and Security Cooperation
PAL	Payments Association of Lesotho
PAN	Payment Association of Namibia
PASA	Payments Association of South Africa
PCC	Public Compliance Communication
PCH	Payment Clearing House
PEPs	Politically Exposed Persons
PFMI	Principles for Financial Markets Infrastructures
PIN	Personal Identification Number
PLACH	Port Louis Automated Clearing House
POC	Proof of Concept
PRIMA	Place of the Relevant Intermediary Approach
PS	Payment Systems
PSD	Payment Services in the Internal Market Directive
PSD	Payment System Determination (Namibia)
PSMB	Payment System Management Body
PSO	PCH System Operator (South Africa)
PvP	Payment versus Payment
PSPs	Payment Service Providers
RBA	Risk-based Approach
RCCP	Recommendations for Central Counterparties
RFP	Request for Proposals
RISDP	Regional Indicative Strategic Development Plan
RSA	South Africa
RSSS	Recommendations for Securities Settlement Systems
RTGS	Real Time Gross Settlement
SADC	Southern African Development Community
SADCBA	SADC Bankers Association
SADCC	Southern African Development Coordination Conference
SADC PF	SADC Parliamentary Forum
SAMOS	South African Multiple Option Settlement System
SARB	South African Reserve Bank

SC	Seychelles
SCO	Standing Committee of Officials
SCV	Clearing Value Subsystem (Angola)
SAECH	Swaziland Automated Electronic Clearing House
SEFT	Seychelles Electronic Funds Transfer
SEPA	Single Euro Payments Area
SFIU	Swaziland Financial Intelligence Unit
SIPO	Strategic Indicative Plan for the Organ
SIPS	Systemically Important Payment Systems
SIRESS	SADC Integrated Regional Electronic Settlement System
SLA	Service Level Agreement
SMS	Short Message Service
SO	Strategic Objective
SPTR	Sistema de Pagamentos em Tempo Real (Angola)
SR	Special Recommendation
SSL	Secure Sockets Layer
SSS	Securities Settlement Systems
STC	Credit Transfer Subsystem (Angola)
STP	Straight-through Processing
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIPSS	Swaziland Interbank Payment and Settlement System
T&C's	Terms and Conditions
TAs	Technical Agreements
TACH	Tanzania Automated Clearing House
TARGET	Trans-European Automated Real-time Gross Settlement System
TBA	Tanzania Bankers Association
TIACH	Truncated Image Automated Clearing House (Seychelles)
TISS	Tanzania Inter-Bank Settlement System
TR	Trade Repositories
TZ	Tanzania
UNCITRAL	United Nations Commission on International Trade Law
UNSC	United Nations Security Council
USD	United States Dollar
USSD	Unstructured Supplementary Service Data
VPN	Virtual Private Network
ZECHL	Zambia Electronic Clearing House Limited
ZETSS	Zimbabwe Electronic Transfer and Settlement System
ZIPSS	Zambian Inter-bank Payment and Settlement System
ZM	Zambia
ZW	Zimbabwe

REFERENCES

- Alliance for Financial Inclusion (AFI) and Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2013 *Public and Private Sector Surveys Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices*
- Bagshaw D 2013 *Arbitration as a Tool for Strengthening Cross-Border Deals: Making a Case for the Harmonisation of Arbitration Laws in the SADC Region* Lilongwe, Malawi
- Bankable Frontier Associates 2012 *Mapping the Retail Payment Services Landscape: Zambia*
- Bank of Mauritius 2011 *Legal Framework of the Domestic Payment System of Mauritius*
- Beswick C *Distributing Cash Through Bank Accounts Save the Children's Drought Response in Swaziland*
- Bilal 2005 *Can the EU Be a Model of Regional Integration? Risks and Challenges for Developing Countries*
- Cirasino M and Garcia J 2008 *Measuring Payment System Development*
- Central Bank of Lesotho "The Southern African Development Community Integrated Regional Settlement System (SIRESS): What? How? Why?" 2013 *CBL Economic Review* (145)
- Commission of the European Communities 2006 *Evaluation Report on the Settlement Finality Directive 98/26/EC (EU 25)* Brussels
- De Koker L 2011 Aligning Anti-Money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when FATF Standards are Clarified *Journal of Financial Crime*, vol. 18, no. 4
- De Koker L and Symington J 2011 *Conservative Compliance Behaviour Drivers of Conservative Compliance Responses in the South African Financial Services Industry*
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2012 *Mutual Evaluation Report: Republic of Angola*
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2007 *Anti-Money Laundering and Combating the Financing of Terrorism Mutual Evaluation/Detailed Assessment Report: Republic of Botswana*
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2011 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Kingdom of Lesotho*
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2008 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: The Republic of Mauritius*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2011 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Republic of Mozambique*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2007 *Mutual Evaluation/Detailed Assessment Report Anti Money Laundering and Combating the Financing of Terrorism: Republic of Namibia*

See Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2008 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: The Republic of Seychelles*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2009 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: South Africa*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (February 2010) Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Kingdom of Swaziland

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) (December 2009) *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: United Republic of Tanzania*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2008 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Republic of Zambia*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 2008 *Mutual Evaluation / Detailed Assessment Report Anti-Money Laundering and Combating the Financing of Terrorism: Republic of Zimbabwe.*

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the World Bank 2008 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: The Republic of Malawi*

European Commission DG Internal Market and Services (DG MARKT) 2013 *Additional Research to Assess the Impact of Potentially Changing the Scope (Art. 3) of the Regulation on Information Accompanying Transfers of Funds*

European Payments Council 2009 *Making SEPA a Reality: The Definitive Guide to the Single Euro Payments Area*

Faria J "Legal Harmonisation Through Model Laws: The Experience of the United Nations Commission on International Trade Law (UNCITRAL)" 2005

Financial Action Task Force (FATF) 2013 *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*

Financial Action Task Force, Asia/Pacific Group on Money Laundering and the World Bank 2013 *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*

Juri G "Out of Africa" 2011 *CLEARIT: The Swiss Professional Journal of Payment Traffic* 47

Kokkola T *The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem* (2010)

- Langhan S and Kilfoil K 2011 *The Cross-border Money Transfer Experience Why Taxis and Buses are Still Preferred to Banks*
- Le Sar B and Porteous D 2012 *Introduction to the National Payments System*
- Magadza M 2009 *Judges Welcome SADC Model Law on HIV/AIDS*
- Mambi *Presentation on E-Transaction and E-Commerce Assessment Report* 2012
- Mathijssen P A *Guide to European Union Law* (2004)
- Mugarura *The Mechanisms for Harmonisation of Global Anti-money Laundering Laws: An Institutional Framework*
- Musavenga T 2011 *The Proposed SADC Parliament: Old Wine in New Bottles or an Ideal Whose Time Has Come?*
- Opping, R 2011 *Legal Aspects of Economic Integration in Africa*
- Parliamentary Counsel's Office 2011 *How to Read Legislation, A Beginner's Guide*
- Rambure D and Nacamuli N *Payment Systems: From the Salt Mines to the Board Room* (2008)
- Reserve Bank of Malawi 2007 *Payment Systems Annual Report*
- Reserve Bank of Malawi 2011 *National Payment System Annual Report*
- SADC Country Progress Report on Lesotho National Payment System for Period April 2011 to March 2012*
- Secretariat of the Committee of Central Bank Governors in SADC 2013 *SADC Financial Systems: Structures, Policies and Markets*
- Southern African Development Community (SADC) Payment Clearing and Settlement Subcommittee 2011 *SADC Payment System Integration using the Common Monetary Area as Proof of Concept*
- Tetley S 1999 *Mixed Jurisdictions: Common Law vs Civil Law (Codified and Un-codified) (Part I)*
- The Banking Enquiry 2008 *Report to the Competition Commissioner by the Enquiry Panel*
- Tsa Tuelano - The Botswana National Payment System Newsletter, Volume 5, 2010*
- United Nations Commission on International Trade Law (UNCITRAL) 2009 *Promoting Confidence in Electronic Commerce: Legal Issues on International use of Electronic Authentication and Signature Methods*
- Volker W *Essential Guide to Payments An Overview of the Services, Regulation and Inner Workings of the South African National Payment System* (2013)
- Wandhöfer R *EU Payments Integration: The Tale of SEPA, PSD and Other Milestones Along the Road* (2010)

Williams M *Pilot Plan to Harmonise Payment Infrastructure in Southern Africa*

Conventions, Model Laws and other International Soft Laws and Principles

Bank for International Settlements Committee on Payment and Settlement Systems 2001 *Core Principles for Systemically Important Payment Systems*

Bank for International Settlements and International Organization of Securities Commissions 2012 *Principles for Financial Market Infrastructures*

Bank for International Settlements and International Organization of Securities Commissions 2004 *Recommendations for Central Counterparties*

Bank for International Settlements and International Organization of Securities Commissions 2001 *Recommendations for Securities Settlement Systems*

Bank for International Settlements and The World Bank 2007 *General Principles for International Remittance Services*

Financial Action Task Force 2012 *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The Recommendations*

Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary (Concluded 5 July 2006)

New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958

UNCITRAL Convention on International Bills of Exchange and International Promissory Notes, 1988

UNCITRAL Model Law Model Law on Electronic Commerce 1996

UNCITRAL Model Law on Electronic Signatures 2001

UNCITRAL Model Law On International Credit Transfers, 1992

UNCITRAL Model Law on International Commercial Arbitration 1985

EU Treaties, Regulations and Directives

Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems

Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on Financial Collateral Arrangements

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services

in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC

Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 Establishing Technical and Business Requirements for Credit Transfers and Direct Debits in Euro and Amending Regulation (EC) No 924/2009

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 On Information on the Payer Accompanying Transfers of Funds

Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 On Crossborder Payments in the Community and Repealing Regulation (EC) No 2560/2001

SADC Treaties, Protocols and Documents

Regional Indicative Strategic Development Plan

Protocol on Finance and Investment (FIP)

Protocol on Finance and Investment Annex 6: Anti-Money Laundering (Unpublished)
Treaty of the Southern African Development Community

SADC Member States: Legislation, Regulations, Directives, Guidelines and Guidance Notes