Making financial markets work for the poor

AML/CFT and Financial Inclusion in SADC

Consideration of Anti-Money Laundering and Combating the Financing of Terrorism Legislation in Various Southern African Development Community (SADC) countries

Lesotho Country Report

Finalised by: Compliance & Risk Resources

March 2015

Contents

LESOTHO COUNTRY REPORT

FinMark Trust, an independent trust based in Johannesburg, South Africa, was established in 2002, and is funded primarily by UKaid from the Department for International Development (DFID) through its Southern Africa office. FinMark Trust's purpose is 'Making financial markets work for the poor, by promoting financial inclusion and regional financial integration' as well as institutional and organisational development, in order to increase access to financial services for the un-served and under-served.

While the underlying focus of this report is on the harmonisation and calibration of provisions found in Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) laws and regulations in the Southern African Development Community (SADC), it is hoped that the country reports will become "living documents" that will be used as a resource for SADC Member States to make appropriate amendments to their domestic laws and regulations, define the strategic direction to achieve the objectives of Annex 12 of the FIP and prompt further research and other initiatives that will support State Parties in fulfilling their harmonisation objectives.

FinMark Trust commissioned Compliance &Risk Resources to conduct the final review of the report and to circulate the report to country stakeholders in order to obtain support and facilitate finalisation. The initial research that informed this country report was conducted and prepared by Sarah Langhan and Associates. Raadhika Sihin assisted in reviewing and editing the initial research and country report. She was assisted by a panel of technical experts comprising of Ben Musuku (World Bank), Tom Malikebu (ESAAMLG) and Prof Louis de Koker (Deakin University, School of Law, Faculty of Business and Law) who reviewed and provided guidance on the content for the initial edited research report.

The authors are grateful for the level of cooperation and assistance provided by all persons consulted during the research phase of the project. We especially acknowledge the willingness of those who made themselves available, often at very short notice, in all participating countries to answer questions, provide numerous documents and generally provide the information that was requested. In this regard, we acknowledge and thank all those who assisted.

1. Changes to the Legal and Regulatory Framework in Lesotho Post 2010

The Eastern and Southern Africa 'Anti-Money' Laundering Group (ESAAMLG) Mutual Evaluation[1] for Lesotho was based on the laws, regulations and other materials supplied by Lesotho, as well as information obtained by the evaluation team during the in-country visit which took place from 29 November 2010 to 10 December 2010. Since the time of the evaluation, an important piece of legislation, the Financial Institutions Act, 2012[2] has been passed. This Act repeals and replaces the Financial Institutions Act 1999 (which was used by the ESAAMLG evaluation team). The Act provides for the authorisation, supervision and regulation of banking and non-banking financial institutions, agents of financial institutions and ancillary financial service providers, and has direct relevance to the AML regime. Companies Regulation was issued in 2012 under s185 of Companies Act, 2011. Despite the fact that the National Payment System Bill has yet to be passed by parliament[3], the Central Bank of Lesotho issued Mobile Money Guidelines in 2012 in terms of s6 (h) of the Central Bank Act, 2000.[4]

The ESAAMLG Mutual Evaluation has led to the compilation of a full list of criminal offences, which indicates the statutes under which they are covered. However, as indicated in the ESAAMLG Mutual Evaluation Report, common law offences are not codified and do not have prescribed sentencing provisions, which creates uncertainty in determining what constitutes a predicate offence to money laundering.

Table 1: Lesotho: Legislation, Regulation Guidelines (Post ESAAMLG Evaluation)

Year	New Legislation, Regulation and Guidelines
In-country Assessment Nov –Dec 2010 **Adopted 2011**	• Financial Institutions Act 3 of 2012 • Companies Act 2011 • Guidelines on Mobile Money, 2013 • *Payment Systems Bill, 2013* • Penal Code 2012 • Money Laundering and Proceeds of Crime (Amendment of Schedule) Notice No. 30 of 2013 • *Money Laundering and Proceeds of Crime (Amendment) Bill, 2014* • Money Laundering (Accountable Institutions) Guidelines 2013 Notice 55 of 2013 • Money Laundering (Prescription of Form) Notice No. 53 of 2013 (Threshold Transactions Reporting Form) • Money Laundering (Prescription of Form) Notice No. 54 of 2013 (Suspicious Transactions Reporting Form) • Money Laundering (Prescription of Reporting Period) Notice No. 69 of 2013 • Financial Institutions (Money Transfer) Regulations No. 14 of 2014 • Declaration of Currency No. 34 of 2014

[1] See 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.*

[2] Act 3 of 2012.

[3] Representatives of the National Payment System Division of the Central Bank of Lesotho indicated during a meeting in February 2013 that the Bill had been held up at the Office of Parliamentary Council (OPC) for over 6 years.

[4] Act 2 of 2000.

2. Current AML/CFT Legislation and Regulation in Force in Lesotho

Table 2 below provides an overview of the current laws, regulations, exemptions, guidelines and guidance notes in force in Lesotho as of June 2014. The legislation is broken up into primary legislation (having a direct bearing on AML/CFT), additional relevant legislation (this covers laws and regulations that impact upon the AML/CFT legal and regulatory framework), laws and regulations applicable to banks, non-bank financial institutions (NBFIs), designated non-financial businesses or professions (DNFBPs) and non-profit organisations. The primary piece of legislation in place is the Money Laundering and Proceeds of Crime Act, 2008[5]. Money Laundering (Accountable Institutions) Guidelines, Money Laundering (Prescription of Form) Notice No.53 of 2013 (Threshold Transactions Reporting Form), Money Laundering (Prescription of Form) Notice No. 54 of 2013 (Suspicious Transactions Reporting Form, Money Laundering (Prescription of Reporting Period) Notice No. 69 of 2013, and Declaration of Currency No. 34 of 2014 have been issued under this Act. The Financial Institutions (Anti-Money Laundering) Guidelines were issued in 2000 under the previous Financial Institutions Act 1999.[6] These were issued by the Central Bank of Lesotho (CBL) before the creation of the FIU.

Table 2: The AML/CFT Regulatory Landscape in Lesotho as of June 2014

	Core Acts		Issued Under the Act
✓	Money Laundering and Proceeds of Crime Act 4 of 2008	✓	• Money Laundering (Accountable Institutions) Guidelines Notice 55 of 2013 • Money Laundering (Prescription of Form) Notice No.53 of 2013 (Threshold Transactions Reporting Form) • Money Laundering (Prescription of Form) Notice No. 54 of 2013 (Suspicious Transactions Reporting Form, • Money Laundering (Prescription of Reporting Period) Notice No. 69 of 2013 • Declaration of Currency No. 34 of 2014
✗	CFT Law	✗	
	Additional Relevant Legislation		
✓	Prevention of Corruption and Economic Offences Act 1999	✗	
✓	Criminal Procedure and Evidence Act 9 of 1981 (As Amended)	✗	
✓	Dangerous Drugs of Abuse Act 5 of 2008	✗	
✓	Anti-trafficking in Persons Act 1 of 2011	✗	
✓	Sexual Offences Act 29 of 2003	✗	
✓	Customs and Excise Act 10 of 1982	✗	
✓	Exchange Control Order 1987	✓	• Exchange Control Regulations 1989
✓	Interpretation Act 19 of 1977	✗	
✗	Mutual Legal Assistance in Criminal Matters Act	✗	
✓	The Fugitive Offenders Act 37 of 1967	✗	
✓	Penal Code Act No. 6 of 2012		
	Legislation Applicable to Banks		
✓	Central Bank of Lesotho Act 2 of 2000	✗	
✓	Financial Institutions Act 3 of 2012	✓	Issued Under Previous Act

[5] Act 4 of 2008.
[6] Repealed by the Financial Institutions Act 3 of 2012.

				• Financial Institutions (Licensing Requirements) Regulations 1999 • Financial Institutions (Internal Control Systems) Regulations 2000 • Financial Institutions (Minimum Local Asset Requirements (Amendment) Regulations 2002 • Financial Institutions Ancillary Financial Service Providers) (Licensing Requirements) Regulations 2003 Issued under the 2012 Act • Financial Institutions (Money Transfer) Regulations No. 14 of 2014
●	National Payment System Bill			
	Legislation Applicable to NBFIs			
✓	Insurance Act 18 of 1976		✗	
✓	Money Lenders Order 1989		✗	
✗	Securities Act		✗	
	Legislation Applicable to DNBPs and NPO's			
✓	Casinos	Casino Order 1989	✓	• Casino Regulations 1990
✓	Lawyers	The Law Society Act 1983 The Legal Practitioners Act 1983	✓	• Law Society Rules 2012
✓	Accountants	The Accountant Act 1977	✗	
✓	Precious Metals and Stones Dealers	The Precious Stones Order 1970	✗	
✗	Estate Agents		✗	
✓	NPOs	The Societies Act 1966	✓	• The Societies Rules 1967

3. Lesotho's Approach to Recommendation 10: Customer Due Diligence (CDD)

CDD requirements are found in sections 16(1), 17(2) and 26 of the Money Laundering and Proceeds of Crime Act, 2008.[7]

3.1 When is CDD required in Lesotho?

Accountable institutions are required, as set out in the Money Laundering and Proceeds of Crime Act, 2008 to obtain information on the purpose and nature of the business relationship when establishing such [section 16(1)(a)], and to adequately identify natural persons and verify their identity by obtaining:

(i) The person's name, address and occupation; and
(ii) The national identity card, passport or other applicable official identifying document.[8]

If the transaction is conducted by a legal entity, the accountable institution is required to adequately identify and verify its legal existence and structure, including information relating to: (i)

[7] Act 4 of 2008.
[8] Section 16(1)(b).

the customer's name, legal status, address and directors; (ii) the principle owners, beneficiaries and control structure; (iii) provisions regulating the power to bind the entity; and to verify that any person purporting to act on behalf of the customer is so authorised, and to identify those persons (section 16(1)(c).

In line with the Financial Action Task Force (FATF) Recommendation 10, accountable institutions are also required to undertake CDD measures when a customer is carrying out an electronic funds transfer, and where there is suspicion of a money laundering offence or the financing of terrorism, and where the accountable institution has doubts about the veracity or adequacy of the customer identification and verification documentation or information it has previously obtained.[9] It must be noted however that although electronic wire transfers are mentioned, there is no specific reference to wire transfers. In this regard, ESAAMLG notes that "there is no law or regulation that requires accountable institutions to conduct customer due diligence when the customer is carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR.VII." 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".[10] In practice however, banks obtain information on the identity of "walk-in" customers who conducts transactions in the bank even though the customers do not maintain an account with the bank.

The threshold approach is introduced in section 16(4) of the Money Laundering and Proceeds of Crime Act (MLPCA), 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.[11] This section is supported by section 16(9)(d) of the Money Laundering and Proceeds of Crime Act, 2008[12] that provides an 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."

This threshold is very low, and is overly cumbersome as it refers to ANY cash transaction and places undue pressure on accountable institutions.

Section 17(2) and section 26 of the Money Laundering and Proceeds of Crime Act, 2008 explicitly prohibit the keeping of accounts in fictitious names. Whilst keeping of an account in an anonymous name is not spelled out in the law, the wording of section 17(2) which reads "customer accounts of an accountable institution shall be kept in the true name of the account holder" is drafted broadly enough to infer that anonymous accounts are prohibited. Section 26(1) of the Money Laundering and Proceeds of Crime Act, 2008 places the liability for using a false name or a fraudulent document when opening an account with the individual involved and the penalty for opening an account using a false name or fraudulent document is imprisonment for a period not exceeding 10 years, or a fine not less than M50, 000 or both. Section 26(2) of the Money Laundering and Proceeds of Crime Act,

[9] Section 16(2).

[10] 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 85.*

[11] M100,000 is equivalent to USD 8278.14 (31/03/2015)

[12] Act 4 of 2008.

2008 however requires the court to have regard to all circumstances of the case, including such custom and practice as may from time to time be current in the relevant trade, business, profession or employment. The court may also take account of any relevant guidance adopted, approved by a public authority acting in the public interest, supervisory function in relation to the accountable institution, or any other body that regulates or is representative of any trade, business, profession or employment, carried on by that person. 26(3)(b) of the Money Laundering and Proceeds of Crime Act, 2008 extends the requirement to accountable institutions which also commit an offence when failing to comply with the provision and are liable, upon conviction, to a fine of not less than M250,000.

3.2 Identification measures and verification sources

Section 16(1) of the Money Laundering and Proceeds of Crime Act, 2008 reads:

"An accountable institution shall-
(a) When establishing a business relationship, obtain information on the purpose and nature of the business relationship;
(b) If the transaction is conducted by a natural person, adequately identify and verify his or her identity, including information relating to: (i) the person's name, address and occupation; (ii) the national identity card or passport or other applicable official identifying document."

We do not agree with the ESAAMLG Mutual evaluation assessors who state that "there is no direct obligation in law or regulation that requires accountable institutions to identify customers when establishing a business relationship. In terms of s16(1)(a), accountable institutions should, when establishing business a relationship only obtain information on the purpose and nature of the business relationship, and not information relating to the identity of the customer such as the person's names and physical address. There are however obligations in s16 (1) (b) for accountable institutions to identify all customers (including existing customers) whenever they conduct a transaction. In this situation, accountable institutions must obtain information on: i) the person's name, address and occupation; and ii) the national identity card or passport or other applicable official identifying documents." We maintain that the intention of the drafters when using the words **"the transaction"** in section 16(1)(b) was to refer to the action of creating a business relationship with a natural person. As such, what is required is the person's name, address and occupation as well as the person's national identity card, passport or other applicable official identifying document."[13]

The Financial Institutions (Anti-Money Laundering) Guidelines, 2000 supports this reasoning as section 6(2) and 6(3) specifically states that:

"Financial institutions are required to identify, on the basis of an official or other reliable identifying document and record, the identity of their customers, either occasional or usual, when establishing business relations or conducting transactions.

(3) Without derogating from the generality of sub-guideline (2), that sub-guideline shall apply, in particular-
    (a) To the opening of accounts or passbooks;
    (b) To fiduciary transactions;

[13] Section 16(8)(a) reads: "The Minister may, acting on the advice of the Authority and the Central Bank, prescribe the official or identifying documents, or the reliable and independent source documents, data or information source documents, data or information or other evidence that is required for identification or verification of any particular customer or class of customers."

(c) To the renting of safe-deposit boxes;
(d) To the use of safe custody facilities; and
(e) To large cash transactions."

The ESAAMLG Mutual Evaluation states "there is no law or regulation which requires accountable institutions to identify and verify the beneficial owner using relevant information or data obtained from a reliable source, such as that the accountable institution is satisfied that it knows who the beneficial owner is."[14] Once again, we do not agree with this statement as section 16(1)(c) reads "(c) if the transaction is conducted by a legal entity, adequately identify and verify its legal existence and structure, including information relating to: (i) the customer's name, legal status, address and directors; (ii) the principle owners and beneficiaries and control structure; (iii) provisions regulating the power to bind the entity; and to verify that any person purporting to act on behalf of the customer is so authorised, and identify those persons." Again, the words "the transaction" is used and not "a transaction" and as such. We maintain that the intention of the drafters was to refer to the "establishment of a business relationship" as the "transaction" in question.

The Money Laundering and Proceeds of Crime Act, 2008[15] does not contain any direct obligation for an accountable institution to conduct ongoing CDD or to ensure that documents, data or information collected under the CDD process is kept up to date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships. Section 21 of the Money Laundering and Proceeds of Crime Act, 2008 does however require an accountable institution to pay special attention to all complex, unusual or large transactions and all unusual patters of transactions, which have no apparent economic or visible lawful purpose.[16]

Section 10 of the Financial Institutions (Anti-Money Laundering) Guidelines, 2000 does however require financial institutions to "review and properly document the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose."

3.3 Timing of verification of identity

Whilst section 16 of the Money Laundering and Proceeds of Crime Act, 2008 requires accountable institutions to undertake CDD when establishing a business relationship, carrying out an electronic funds transfer, where there is suspicion of a money laundering offence or the financing of terrorism, for cash transactions over M100, 000 and where the accountable institution has doubts about the veracity or adequacy of the customer identification and verification documentation, the Money Laundering and Proceeds of Crime Act, 2008 does not contain any provisions related to the completion and verification of CDD as soon as reasonably practicable following the establishment of the relationship. The Money Laundering and Proceeds of Crime Act, 2008 is also lacking a provision stating that if an accountable institution cannot comply with their CDD obligations, they should not open an account, commence business relations or perform the transaction, and should terminate the business relationship. Nonetheless, these short-comings have been addressed under

[14] 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* 87.
[15] Act 4 of 2008.
[16] This is repeated in Section 10 of the Financial Institutions (Anti-Money Laundering) Guidelines, 2000 which requires financial institutions to "review and properly document the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose."

the Money Laundering and Proceeds of Crime (Amendment) Bill. It is anticipated that the Bill will be promulgated in 2015.

3.4 Risk-based approach to CDD: Simplified Measures

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 risk customers. Financial institutions are required to split customer risk levels, as set out in table 3 below. The KYC Guidelines do not mandate the application of simplified or reduced CDD measures by financial institutions to customers on a risk sensitive basis, although low risk customers are classified as per Table 3 below.

Table 3: Classification of Customers According to Risk Perception

Classification of Customers According to Risk Perception		
Higher Risk	**Medium Risk**	**Low Risk**
Political exposed persons	Business relationship is between 1 year and three years	Customers who are neither high nor medium.
Customer who appears in the office of foreign assets committee listing	The remaining non-resident customers who are not high risk customers	Individuals with a gross monthly income of M4, 999.99 and below
Customers from countries not implementing or insufficiently applying the FATF Standards	An individual earning a gross monthly income of M5 000. 00 and M2, 999.999.99	Legal entities whose gross monthly income is between M499, 999.99 and below
Correspondent banks	Sole proprietor subject to verification of personal capacity and source of income	

The current requirement that each customer or potential customer must provide a street address in Lesotho and a recognised form of identification is generally problematic as many people live in areas that do not have formal street addresses and, in the past, Lesotho has not had an Identification System (formal identification cards).[17] This problem was exacerbated by the fact that the Voter Registration Card, which was initially accepted as an acceptable form of identification, is no longer accepted. Formal Identification Cards were introduced from the 3rd July, 2013. The system is such that all citizens have to register their births, irrespective of the birth certificates previously issued. For those above 16 years of age, they are issued with IDs immediately after being issued with a new birth certificate. The process is still unfolding, though it halted at some stage when there were issues concerning contractual obligations between the issuing Authority and the service provider producing the necessary documents. It follows that not all citizens have been issued with IDs.

[17] Section 16(1)(a).

According to the FIU, "the current Law doesn't provide for a risk-based approach. However, due to the Financial Inclusion agenda, regulators (the Central Bank) apply a risk-based approach to new products. The Mobile Money Guidelines use a risk-based approach."[18] In line with the risk-based approach mandated by FATF Recommendation 10, Appendix 11 of the Lesotho Guidelines on Mobile Money introduces a hierarchical approach towards the implementation of KYC/CDD. The three tier KYC/CDD requirement matrix for mobile money issuers is set out in Table 4 below.

Table 4: Three Tier KYC Requirement

KYC/CDD Level	Verification Requirement	Transaction Limit
LEAST KYC	Full names and surname Phone number Physical address	Daily Limit M2,500 Monthly Limit M10,000
PARTIAL KYC	Full names and surname Phone number Physical address Passport Number	Daily Limit – M5,000 Monthly Limit – M15,000
FULL KYC	AS PER KYC requirements as laid out in the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (2006)[19]	Daily Limit – M7,500 Monthly Limit – M20,000

The above table has been extracted from the Guidelines on Mobile Money, 2012. It is recommended that the reference to "Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (2006)" should be reviewed as this law does exist in Lesotho.

The principle behind the adoption of a tiered approach is sound. However, the application of the above in practice would be compromised if incorrect reference is made to regulatory requirements in question. It is also recommended that the legal standing of the guidelines in question should be considered in the light of the existing regulatory framework that does not provide for a risk-based approach.

4. Lesotho's Approach to Recommendation 11: Record Keeping

Section 39(3)(b) of the Financial Institutions Act, 2012 requires financial institutions to keep records of every transaction that it conducts for a period of at least 10 years after the completion of the transaction. As per section 39(3)(a) of the of the Financial Institutions Act, 2012, "such records may be kept in written form or kept on microfilm, magnetic tape, optical disk, or any other form of mechanical or electronic data storage and retrieval mechanism as the Commission may agree to."[20] This section is in conflict with section 17(1)(a) of the Money Laundering and Proceeds of Crime Act, 2008[21] which only requires an accountable institution to establish and maintain records of suspicious transactions for a period of at least five years from the date the relevant business or transaction was completed, or termination of business relationship, whichever is the later."[22]

[18] This meeting was held with representatives of the FIU in February 2013.
[19] Lesotho does not have a law with this reference. It is presumed that the reference should have been to the Money Laundering and Proceeds of Crime Act 4 of 2008.
[20] S39(3)(a) Act 3 of 2012.
[21] Act 4 of 2008.
[22] S17(1)(a) and s17(4).

Whilst section 17(1)(b) of the Money Laundering and Proceeds of Crime Act, 2008 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, 2012[23] 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. It is noted that the Money Laundering and Proceeds of Crime (Amendment) Bill 2014 requires accountable institutions to keep specified records. Record keeping requirements are also specified in guideline 17 of the Money Laundering (Accountable Institutions) Guidelines 2013.

5. Lesotho's Approach to Recommendation 13: Correspondent Banking

The ESAMMLG Mutual Evaluation report states that "accountable institutions in the Kingdom of Lesotho do not conduct cross-border correspondent banking relationships as cross-border transactions are channeled through foreign subsidiaries of South African banks for clearance by their respective head offices in South Africa. It is noted that since the Kingdom of Lesotho is a member of the Common Monetary Area with South Africa, Namibia and the Kingdom of Swaziland, such transactions are not considered to be cross-border transactions when transferred for clearance in South Africa or to any of the other members of the Area." [24] Regardless of the manner in which these relationships are structured, section 16(5) of the Money Laundering and Proceeds of Crime Act, 2008[25] requires an accountable institution, in relation to its cross-border correspondent banking and other similar relationships, to adequately identify and verify the person with whom it conducts such a business relationship, to gather sufficient information about the nature of the business of the person and to determine from publically available information the reputation of the person and the quality of supervision to which the person is subjected. The accountable institution is also required to assess the person's anti-money laundering and terrorist financing controls, obtain approval from senior management before establishing a new correspondent relationship and document the responsibilities of the accountable institution and the person.[26]

Section 16(6) of the Money Laundering and Proceeds of Crime Act, 2008 deals with payable-through accounts and requires an accountable institution to ensure that the person with whom it has established the relationship has verified the identity of and performed on-going due diligence on such of that person's customers that have direct access to accounts of the accountable institution; and is able to provide the relevant customer identification data upon request to the accountable institution.

The Money Laundering and Proceeds of Crime Act, 2008 does not contain a provision prohibiting accountable institutions from entering into correspondent banking relationships with shell banks. It

---

[23] Act 3 of 2012.
[24] 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* 92.
[25] Act 4 of 2008.
[26] Person is defined in section 2 of the MLPCA as a natural or legal person.

is noted that this prohibition is covered under the Money Laundering and Proceeds of Crime (Amendment) Bill 2014.

The new Financial Institutions Act, 2012[27] does not contain any provisions on correspondent banking. The Payment Systems Bill, 2013 is also silent on the matter.

6. Lesotho's Approach to Recommendation 14: Money Transfer Services

Money Transfer Services are listed as accountable institutions in Schedule 1 to the Money Laundering and Proceeds of Crime Act, 2008 and are subject to the provisions of the Act including CDD and record keeping requirements. The Financial Institutions (Licensing Requirements) Regulations 2003 apply to ancillary financial service providers and set out capital requirements and the licensing procedure by the CBL.[28] Whilst not specifically included in the definition of ancillary financial service providers, it is arguable that money transfer service providers fall under this definition. It is noted in the ESAAMLG Mutual Evaluation report that "only banks have put in place control measures to combat ML or TF through money or value transfer services. However, the same deficiencies identified regarding financial institutions under Section 3 of this report also apply to money or value transfer services provided by banks. Post Office and TEBA have not implemented ML /TF control measures for money or value transfer transactions."[29]

7. Lesotho's Approach to Recommendation 15: New Technologies

There are no provisions contained in any of the relevant financial services related laws in Lesotho pertaining to the potential misuse of new technology. There is also nothing to be found in legally enforceable statutes with respect to requiring accountable institutions to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. It is however encouraging to note that Principle 6 of the Central Bank of Lesotho National Payment System Division Guidelines on Mobile Money, 2012 is entitled "*Implement Adequate Measures to Prevent the Use of Mobile Money for Illegal Activities*" and is AML/CFT focused. Whilst technically not legally enforceable as the document is simply a Guideline and not a regulation or directive which has been gazetted, the document does provide several good risk-management pointers for issuers of mobile money.[30] The Money Laundering and Proceeds of Crime (Amendment) Bill 2014 has provisions requiring accountable institutions to have and implement policies and procedures or measures aimed to prevent the misuse of technological developments in ML and FT schemes.

Principle 6(1) requires an issuer of mobile money to ensure that the design and implementation of its mobile money scheme reduces the opportunities and incentives for abuse and provides a means to filter out suspicious activities. At a minimum, mobile money service providers are required to

---

[27] Act 3 of 2012.

[28] Ancillary financial service providers are defined as "a person who engages in providing auxiliary financial services, other than management of collective investment schemes, such as foreign exchange dealing services, electronic fund transfer services, money market dealing, money market brokerage, private equity fund management, and other similar auxiliary services."

[29] 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* 134.

[30] An issuer of mobile money is defined as "any entity that is responsible for the payment obligation and assumes liabilities for the mobile money issued."

ensure that complete "end-to-end" electronic audit trails are in place and that such audit trails provide a complete record of a) funds received by the merchant, b) funds distributed by the merchant, c) a complete record of all transfers undertaken by the participant, d) a complete record of all funds received by the participant and e) complete electronic records of all funds transfers and recipients undertaken within any service providers products and services that will be available to the regulator as required or on demand.

Issuers are required, in terms of Principle 6(2), to conduct customer due diligence on potential merchants who apply to participate in their scheme and to evaluate the company's background to ascertain that the merchant is both viable and financially sound, with no evidence of criminal or illegal activities. Principle 6(3) states that issuers are required to comply with the Money Laundering and proceeds of Crime Act (MLPCA) 2008, and the relevant regulations pertaining to anti-money laundering and combating the financing of terrorism, although it must be noted that neither "mobile money issuers" nor "mobile network operators" are listed as accountable institutions in Schedule 1 of the MLPCA. A mobile money issuer could however fall under the catch all "a person who carries on the business of money transmission services."

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, including when establishing customer relationships and conducting ongoing due diligence. In addition, there are no requirements for accountable institutions to have specific and effective CDD procedures that are applicable to non-face-to-face customers. The Money Laundering and Proceeds of Crime (Amendment) Bill 2014 has provisions requiring accountable institutions to have and implement policies and procedures or measures to address any specific risks associated with non-face-to-face business relationships or transactions.

8. Lesotho's Approach to Recommendation 16: Wire Transfers

Section 22(1) of the Money Laundering and Proceeds of Crime Act, 2008[31] requires only banks to include accurate originator information and other related messages on electronic funds transfer and other forms of funds transfers. This information is required to remain with the transfer. Section 22(1) does not apply to credit or credit card transactions, provided that the credit or debit card number is included in the information accompanying the payment.[32] Section 22(1) of the Money Laundering and Proceeds of Crime Act, 2008 does also not apply to electronic funds transfers and settlements between banks where the originator and beneficiary of the funds transferred are acting on their own behalf.[33] The Money Laundering and Proceeds of Crime Act, 2008 does not require a Financial institution that identifies incomplete information of sender to reject the transfer or request additional information and/or report such to the FIU, and does not contain the suggested *de minimus* threshold of $1,000.

9. Lesotho's Approach to Recommendation 17: Reliance on Third Parties

Section 16(7)(a) of the Money Laundering and Proceeds of Crime Act, 2008 requires accountable institutions relying on an intermediary or third party to undertake its CDD obligations, or to

[31] Act 4 of 2008.
[32] Section 21(2).
[33] Section 21(3).

introduce business to immediately obtain the required information and documents from the third party, and ensure that copies of identification data and other relevant documentation relating to the requirements are made available by the intermediary or the third party upon request without delay. 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.[34] The Money Laundering and Proceeds of Crime Act, 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. The Money Laundering and Proceeds of Crime (Amendment) Bill 2014 has provisions placing the ultimate liability relating to the aforementioned with the accountable institution.

10. Lesotho's Approach to Recommendation 18: Internal Controls

Sections 19 and 20 of the Money Laundering and Proceeds of Crime Act, 2008 require accountable institutions to establish and maintain internal reporting procedures. These sections are limited in their nature, but section 20 does make reference to "appropriate" measures and "appropriate" training, therefore, arguably the beginnings of the adoption of a risk-based approach. The Money Laundering and Proceeds of Crime Act, 2008 does not contain any specific requirement for accountable institutions to establish and maintain internal procedures, policies and controls that address CDD, record retention, detection of unusual and suspicious transactions to prevent money laundering and the financing of terrorism. The Money Laundering and Proceeds of Crime (Amendment) Bill 2014 has provisions requiring accountable institutions to have and implement policies, procedures, and controls for fighting ML and combating FT. With respect to the requirement to appoint an AML/CFT compliance officer, the Act provides that accountable institutions should identify persons who will ensure compliance with the obligations under the Money Laundering and Proceeds of Crime Act, 2008. As noted in the ESAAMLG Mutual Evaluation report, "this provision appears unclear to the assessors since the word "to identify" does not ordinarily mean "to appoint". Guidelines have been issued to clarify that accountable institutions shall appoint a compliance officer.[35] In addition, the Act stipulates that the identified person must be a senior officer with relevant qualifications and experience to champion AML/CFT activities in terms of s19(2)(a). However, it is not clear whether the senior officer will be at a management level and the term "senior officer" has not been defined. Despite the deficiency in the law, it appears from discussions with representatives of the banking sector that Compliance Officers hold management positions."[36]

No reference is made in the Money Laundering and Proceeds of Crime Act, 2008 to the implementation of group wide programmes against money laundering and terrorist financing, and the requirement to implement policies and procedures for sharing information within the group. The MLPCA is also silent on the FATF recommendation that financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements.

---

[34] Section 16(7)(c).

[35] Guideline 4 of the Money Laundering (Accountable Institutions) Guidelines 2013.

[36] 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* 116.

11. Lesotho's Approach to Recommendation 20: Suspicious Transaction Reports (STRs)

The obligation to report suspicious transactions is set out in sections 18 and 23 of the Money Laundering and Proceeds of Crime Act, 2008. Section 18(1) reads:

"Whenever an accountable institution has reasonable grounds to suspect that any transaction is related to the commission of money laundering offence or terrorist financing, it shall, within the prescribed period after forming that suspicion and wherever possible **before the transaction carried out** -
(a) Take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary;
(b) Prepare a report of the transaction in accordance with subsection (2); and
(c) Communicate the information contained therein to the Unit and Authority in writing or in such other forms as the Minister may from time to time prescribe."

Supervisory authorities are also required to report suspicious transactions to the FIU.[37]

Unfortunately, on the day of the scheduled meeting with the FIU, the legal team was unable to attend the meeting due to being otherwise engaged with training on AML compliance issues. As such, two individuals from Administration and IT were interviewed and were unable to provide answers to several questions posed. The FIU is already receiving STRs and threshold transactions. Accountable institutions use prescribed forms[38] for the purpose. These reports are submitted to the FIU alone, and not the Central Bank or any other authority. The FIU have procured the IMBI2 system (software) and this is already implemented. Suspicious transactions are reported manually. Threshold transactions are reported as encrypted spreadsheets using email.

12. Lesotho's Approach to Recommendation 34: Guidance and Feedback

Section 15(2)(e) of the Money Laundering and Proceeds of Crime Act, 2008 requires the FIU to "issue to banks, accountable institutions and members of relevant professions or occupations, such guidelines as it considers appropriate to combat money laundering and financing of terrorism activities." Money Laundering (Accountable Institutions) Guidelines No. 55 of 2013 have been issued.

13. High Level Recommendations for Lesotho

The recommendations set out in Table D5 below are not intended to be exhaustive. These high level recommendations provide an indication on how specific sections in the Money Laundering and Proceeds of Crime Act, 2008 could be amended to bring the law in line with several of the revised FATF Recommendations.

---

[37] Section 23(1) Act 4 of 2008.

[38] Money Laundering (Prescription of Form) Notice No. 54 of 2013 (Suspicious Transaction Reporting Form) and Money Laundering (Prescription of Form) Notice No. 53 of 2013 (Threshold Transaction Reporting Form).

Table 5: High Level Recommendations for Lesotho

R10	CDD: Component A - When CDD is Required
It is recommended that section 16(4) of the Money Laundering and Proceeds of Crime Act, 2008 be amended to allow for a threshold increase to USD 15,000 and alternative wording should be considered for, "carrying out occasional transactions above the 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."	
R10	CDD: Component B - Identification Measures and Verification Sources
It is recommended that the Authorities consider permitting alternative documents for identification purposes and amending the Law to include a list of acceptable independent verification sources.	
R10	CDD: Component C - The Timing and Verification of Identity
The Money Laundering and Proceeds of Crime Act, 2008 does not contain any provisions related to the completion and verification of CDD, as soon as reasonably practicable, following the establishment of the relationship. The Money Laundering and Proceeds of Crime Act, 2008 is also lacking a provision stating that if an accountable institution cannot comply with their CDD obligations, they should not open an account, commence business relations or perform the transaction and should terminate the business relationship. It is recommended that the authorities consider rectifying these deficiencies as soon as is reasonably practicable.	
R10	CDD: The Risk-Based Approach to CDD - Simplified Measures and Exemptions
CDD measures are the same for all customers in Lesotho, and 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 risk customers. These Guidelines are however not enforceable. The current requirement that each customer or potential customer must provide a street address in Lesotho, and a recognised form of identification, is generally problematic as many people live in areas that do not have formal street addresses and Lesotho does not have a formal Identification System. This problem has been exacerbated by the fact that the Voter Registration Card, which was initially accepted as an acceptable form of identification, is no longer accepted. According to the FIU, "the current Law doesn't provide for a risk-based approach." However, due to a Financial Inclusion agenda, regulators (the Central Bank) apply a risk-based approach to new products. The Mobile Money Guidelines use a risk-based approach. It is recommended that Lesotho specifically introduce the risk-based approach to CDD into law and require financial institutions to determine the extent of customer due diligence measures on a risk sensitive basis depending on the type of customer, business relationship, product or transaction. Reporting entities should also be able to demonstrate to their supervisory authority that the extent of the measures are appropriate in relation to the risks of money laundering, financing of terrorism or other criminal conduct. Additionally, simplified due diligence processes should be specifically provided for in the law that	

allow 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 should be extended to specified low risk products, services, transactions and delivery channels, particularly to products or services that provide appropriately defined and limited services to certain types of customers so as to increase access to financial services. (See South Africa Exemption 17, Circular 6).	
R11	Record Keeping
It is recommended that the inconsistency between section 39(3)(b) of the Financial Institutions Act, 2012 and section 17 of the Money Laundering and Proceeds of Crime Act, 2008 be reviewed and rectified.	
R13	Correspondent Banking
Section 16(5) of the Money Laundering and Proceeds of Crime Act, 2008 is largely compliant with FATF Recommendation 13. The law does not however prohibit banks from entering into or continuing a relationship with a shell bank. It is recommended that the Authorities consider resolving this deficiency as soon as is reasonably practicable.	
R15	New Technologies
There are no provisions contained in any of the relevant financial services related laws in Lesotho pertaining to the potential misuse of new technology. There is also nothing to be found in legally enforceable statutes with respect to requiring accountable institutions to have policies in place, or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. 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. It is recommended that authorities consider resolving this deficiency as soon as is reasonably practicable.	
R16	Wire Transfers
Section 22 of the Money Laundering and Proceeds of Crime Act, 2008 covers electronic funds transfer and other forms of funds transfers, and is largely compliant with FATF Recommendation 16. It is however recommended that authorities consider the inclusion of the suggested de minimus threshold of US$1,000.	
R17	Reliance on Third Parties
Section 16(7)(a) of the Money Laundering and Proceeds of Crime Act, 2008 requires accountable institutions relying on an intermediary or third party to undertake its CDD obligations or to introduce business to immediately obtain the required information and documents from the third party, and ensure that copies of identification data and other relevant documentation relating to the requirements are made available by the intermediary or the third party upon request without delay. 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 MLPCA 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. It is recommended that this should be rectified as soon as is reasonably practicable.	
R18	Internal Controls

Sections 19 and 20 of the Money Laundering and Proceeds of Crime Act, 2008 require accountable institutions to establish and maintain internal reporting procedures. These sections are limited in their nature but section 20 does make reference to "appropriate" measures and "appropriate" training, therefore, arguably the beginnings of the adoption of a risk-based approach. The Money Laundering and Proceeds of Crime Act, 2008 does not contain any specific requirement for accountable institutions to establish and maintain internal procedures, policies and controls that address CDD, record retention, detection of unusual and suspicious transactions to prevent money laundering and the financing of terrorism. With respect to the requirement to appoint an AML/CFT compliance officer, the Act provides that accountable institutions should identify persons who will ensure compliance with the obligations under the MLPCA. As noted in the ESAAMLG Mutual Evaluation report, "this provision appears unclear to the assessors since the word 'to identify' does not ordinarily mean 'to appoint'.[39] In addition, the Act stipulates that the identified person must be a senior officer with relevant qualifications and experience to champion AML/CFT activities in terms of s19(2)(a). However, it is not clear whether the senior officer will be at a management level and the term 'senior officer' has not been defined. Despite the deficiency in the law, it appears from discussions with representatives of the banking sector that Compliance Officers hold management positions."

No reference is made in the Money Laundering and Proceeds of Crime Act, 2008 to the implementation of group wide programmes against money laundering and terrorist financing, and the requirement to implement policies and procedures for sharing information within the group. The Money Laundering and Proceeds of Crime Act, 2008 is also silent on the FATF recommendation that financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements. It is recommended that the authorities consider resolving these deficiencies as soon as is reasonably practicable.

[39] 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* 116.