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

Malawi Country Report

Finalised by: Compliance & Risk Resources

March 2015

Contents

MALAWI 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 and 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 country report, with the assistance of 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).

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 Post March 2008

The World Bank Mutual Evaluation team visited Malawi from 25th February to the 11th March 2008. The final report was approved and published in December 2008.[1] Malawi has enacted several statutes since 2010 that have a direct bearing on the AML/CFT framework. (See Table 1 below.) Several financial services laws were promulgated and others amended in 2010. This was the culmination of several years of work that began under the auspices of the World Bank, the Malawi Government and the FIRST Initiative.[2] As part of its policy response to the noted shortcomings in the financial system in Malawi, the Government embarked on a comprehensive legal and regulatory modernisation programme. From 2010 to 2012, Parliament passed six financial services Acts and the Reserve Bank of Malawi (Amendment) Act, 2011.[3] These Acts are reflected in Table 1 below.

Unfortunately, as noted by representatives of the Reserve Bank of Malawi (RMB) National Payment System Department, at the time when the core financial services legislation was reviewed and new Acts passed, the National Payment System laws were not categorised as a financial services laws and were therefore not included in the modernization programme.[4] The National Payment System Bill has not been enacted, but is currently in the final stages of review. As noted by the NPS Department, "there appears to be willingness and enthusiasm to make sure that the law is passed by the end of the year."[5] Despite the fact that there is currently no legally enforceable National Payment System Act in place which confers upon the RBM the mandate to issue guidelines, in 2011 the RBM made use of its mandate under s4(e) of the Reserve Bank of Malawi (RBM) Act 1989 (as amended) to issue the Guidelines for Mobile Payment Systems, 2011. These Guidelines, which apply only to non-bank based mobile payments models, contain important provisions with respect to customer enrolment and the requirement to meet KYC requirements as laid out in the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act, 2006[6] and the regulations thereto. In addition to the new financial services laws, the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011, were issued by the Minister of Finance under the powers conferred on him by s105 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (Cap. 8:07), in September 2011. In addition to the changes in the legal and regulatory landscape, the FIU has reported that, since the Mutual Evaluation, Malawi has established a National AML/CFT Committee, which is chaired by the Ministry of Finance. In addition, MOU's have been signed between the FIU and the Reserve Bank of Malawi (RBM), the Anti-corruption Bureau and Immigration Department. In May 2013, the FIU were in the process of finalising their relationship with the Malawian Revenue Authority. The Insurance Sector has now been included as

---

[1] 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 Malawi.*

[2] See Kabango G *Key Note Address* Ku Chawe Inn, Zomba Kabango, Deputy Governor, Supervision of Financial Institutions stated that, "A consultancy firm was engaged to carry out an assessment of the financial system in Malawi in 2004 to 2005 through the Financial Sector Regulatory Reforms Programme. The assessment concluded that the financial sector in Malawi was relatively underdeveloped, and that there was a need to institute measures to deepen and broaden the sector so that it could contribute more to economic growth of the country. The report also noted the financial sector to be bank-centric, with very low penetration of non-bank financial products."

[3] Act 5 of 2011.

[4] The National Payment System Department was interviewed in Malawi in May 2013 as part of the research for the SADC Payments Project.

[5] Input has been provided by a number of stakeholders, including the IMF, World Bank, and Ministry of Trade and Ministry of Finance. Additional pressure to make sure that the Bill is passed was created by the introduction of a new Automated Transfer System (ATS) system.

[6] Act 11 of 2006.

a reporting institution, and insurers have been requested to appoint AML/CFT Compliance Officers. Malawi has completed a ML/FT National Risk Assessment.

Table 1: Malawi: Legislation, Regulation Guidelines (Post Mutual Evaluation)

Year	Legislation, Regulation Guidelines (Post Mutual Evaluation)
In-country Assessment Feb - March 2008 Adopted 2008	• Insurance Act 9 of 2010 • Banking Act 10 of 2010 • Credit Reference Bureau Act 18 of 2010 • Securities Act 20 of 2010 • Microfinance Act 21 of 2010 • Financial Services Act 26 of 2010 • Police Act 12 of 2010 • Pensions Act 6 of 2011 • Reserve Bank of Malawi (Amendment) Act 5 of 2011 • Guidelines for Mobile Payment Systems, 2011 • Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 • *The Payment Systems Bill, 2010*

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

Table 2 below provides an overview of the current laws, regulations, exemptions, guidelines and guidance notes in force in Malawi 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 AML/CFT Act in place in Malawi is the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and its supporting regulations issued in 2011.[7]

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

	Core Acts		Issued Under the Act	
✓	Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act 11 of 2006		✓	• Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011
	Additional Relevant Legislation			
✓	Corrupt Practices Act of 1996		✗	
✓	The Penal Code 1930		✗	
✓	Police Act 12 of 2010		✗	
✓	Dangerous Drugs Act of 1956		✗	
✓	Criminal Procedure and Evidence Code 1968		✗	
✓	Customs and Excise Act 13 of 1969		✗	
✓	Exchange Control Act of 1989		✗	
✓	Companies Act of 1984		✗	
✓	Business Name Registration Act of 1968		✗	

[7] Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.

✓	Trustees Incorporation Act 5 of 1962			✘	
✓	Trustees Act 24 of 1967			✘	
✓	Mutual Assistance in Criminal Matters Act of 1991			✘	
✓	Extradition Act 9 of 1968			✘	
	Legislation Applicable to Banks				
✓	Reserve Bank of Malawi Act [Chapter 44:02] of 1989 (As Amended)[8]			✘	
✓	Banking Act 10 of 2010			✓	Directive No D01-2005/CDD Customer Due Diligence for Banks and Financial Institutions
✓	Financial Services Act 26 of 2010			✘	
●	The Payment Systems Bill, 2014			✘	
	Legislation Applicable to NBFI's				
✓	Financial Services Act 26 of 2010			✘	
✓	Securities Act 20 of 2010			✘	
✓	Insurance Act 9 of 2010			✘	
✓	Pensions Act of 2011				
✓	Microfinance Act of 2010				
✓	Financial Cooperatives Act of 2011				
✓	Cooperative Society's Act of 2010				
✓	Credit Reference Bureau Act of 2010				
	Legislation Applicable to DNBPs and NPO's				
✘	Casinos			✘	
✓	Lawyers	Legal Education and Legal Practitioners Act 20 of 1965		✘	
✓ ●	Accountants	Public Accountants and Auditors Act of 1982 Public Accountants and Auditors Bill 2013		✘	
✓	Precious Metals and Stones Dealers	Mines and Minerals Act of 1981		✘	
✘	Estate Agents			✘	
✓	NPOs	Non-Governmental Organisations Act of 2000		✘	

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

CDD requirements are found in sections 24 to 26 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[9] and Regulations 3 to 22 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011. Customer Due Diligence Requirements are also set out in section 100 of the Financial Services Act, 2010.[10]

[8] See Reserve Bank of Malawi (Amendment) Act 5 of 2011.
[9] Act 11 of 2006.
[10] Act No. 26 of 2010.

3.1 When is CDD required in Malawi?

Section 24(1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[11] requires every financial institution before entering into a business relationship with a customer to "ascertain the identity of the customer or beneficial owner on the basis of an official or other identifying document."[12] Financial institutions are also required to 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 entering into a continuing business relationship, or, in the absence of a business relationship, conducting any transaction, carrying out an electronic funds transfer, where there is a suspicion of money laundering offence or the financing of terrorism, or the financial institution has doubts about the veracity or adequacy of the customer identification and verification documentation or information it had previously obtained.

It is important to note that section 24(1)(a)(ii) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[13] 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 which requires a financial institution to establish the identity of every customer when -

"(a) Establishing a continuing business relationship;
(b) In the absence of a continuing business relationship, conducts any transaction exceeding K500,000;[14]
(c) Carrying out several transactions within fourteen days, which appear to be linked and when consolidated, add up to K500,000;
(d) Carrying out an electronic funds transfer;
(e) There is a suspicion of money laundering or terrorist financing, irrespective of any exemptions or threshold that are referred to elsewhere in these Regulations; or
(f) The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data."[15]

[11] Act 11 of 2006.
[12] Financial institution is very broadly defined in the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and includes a number of DNFBPs in the definition. Accountable institutions should be split into banks, NBFIs and DNFBPs. In this regard, the Mutual Evaluation report notes that "the definition of the term financial institution used in the ML & TF Act is the same as the definition of that term provided in the Glossary to the FATF 40 Recommendations on Money Laundering (FATF 40), except that it does not include insurance company functions. In addition, the definition of financial institution used in the ML & TF Act includes designated non-financial businesses and professions (DNFBPs), as described in the Glossary to the FATF 40. Thus, for purposes of the all compliance requirements under the ML & TF Act in Malawi, there is no distinction between financial institutions and DNFBPs; both are covered by the same requirements that are applicable to financial institutions, except that insurance companies are not at all by the statute."
[13] Act 11 of 2006.
[14] This is equivalent to USD 1142.49(31/03/2015).
[15] Regulation 3(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.

All the requirements set out in the Financial Action Task Force (FATF) Recommendation 10 are addressed in Regulation 3(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 although it must be noted that the threshold of K500,000 is equivalent to USD1,142.49, is extremely low and well below the designated threshold of USD15,000 set in the FATF Recommendation. This low threshold adversely impacts upon financial inclusion opportunities. It is understood that this was set taking into account the unique circumstances in the Malawi economy. It currently has a cash economy and such regulations are put in place to reduce the reliance on cash transactions. However, the regulatory authorities have reasoned that using the full USD15,000 threshold would represent a relatively high ML/CTF risk. Malawi has undertaken a ML/TF national risk assessment and the threshold is determined in the light of the outputs thereof.

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.

Section 24(2)(c) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 requires the financial institution to adequately identify and verify the legal existence and structure of legal persons by acquiring information on (i) the name, legal form, address and directors of the entity, (ii) the principal owners, beneficiaries and control structure of the entity, (iii) provision regulating the power to bind the entity, and verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.

There is a significant discrepancy between the section 24(10) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and section 100(4) of the new Financial Services Act, 2010[16] with respect to the pecuniary penalty applicable to financial institutions which fail to undertake CDD measures.[17] Section 24(1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[18] reads:

"A person who contravenes this section shall be liable
(a) In the case of a fine natural person, to imprisonment for two years and to a fine of K100,000; or
(b) In the case of a corporation, to a fine of K500,000 and loss of business authority."

Section 100(4) of the Financial Services Act, 2010[19] reads:

"Any director, manager, officer or employee of a financial institution who makes or permits to be made any transaction, including the opening of an account –

(a) Without taking all reasonable steps to establish the true identity of the person concerned in the transaction;
(b) When he has doubts or has reason to doubt the authenticity of documents and the truth of written or oral statements material to the transaction; or
(c) When he knows or has reason to suspect that any of the funds involved in the transaction have been obtained by any party as the direct or indirect result of an activity that is illegal inside or outside Malawi, commits an offence, and shall, on conviction be liable to a fine of five million Kwacha (K5, 000,000) and to imprisonment for two years."

[16] Act 26 of 2010.
[17] Act 26 of 2010
[18] Act 11 of 2006.
[19] Act 26 of 2010.

There is therefore a discrepancy in the level of the applicable fine in the amount of K4,900,000 when compared with the fine for natural persons. It is also interesting to note that section 100(4)(c) of the Financial Services Act, 2010 does not refer to the fine which is applicable to the financial institution or the potential loss of business authority / license.

Both section 26(2) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[20] and Regulation 3(2) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 prohibit the opening, operation and maintenance of anonymous accounts and accounts in fictitious, false and incorrect names. Financial institutions are also required to report the matter to the FIU if it discovers that a business relationship has been established or that the single transaction has been conducted using a fictitious, false or incorrect name.[21]

Financial institutions are also required, when establishing a business relationship, to obtain information on the purpose and nature of the business relationship. In the case of a natural person, financial institutions are required to adequately identify and verify the identity of the person, including information relating to – (i) the name, address and occupation of the person, (ii) the national identity card or passport or the applicable official identifying document of the person, and take reasonable measures to establish the source of wealth and property of the person.[22]

Regulation 3(4) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 specifically states that a financial institution shall use a risk-based approach to identify (a) non-resident customers; (b) private banking customers; (c) legal entities; (d) public officials; (e) a customer who has been refused banking services by another institution; and (f) other forms of high risk categories of customers, beneficial owners, beneficiaries, or business relationships.

3.2 Identification measures and verification sources

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;
(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."

[20] Act 11 of 2006.
[21] Regulation 3(3) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.
[22] Section 24(2) Act 11 of 2006.

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 Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 presents problems for banks and other NBFIs. 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.[23] Regulation 4 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 allows for alternative means of providing one's 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." People live in areas that do not have street names and to avoid excluding such people from the formal financial system, alternative address verification measures may be used. For example, a person could describe the location or draw a map of where they stay. 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 using a risk-based approach, i.e. they would largely be applicable in respect of lower risk clients. The Regulation also makes use of the words "where applicable" with respect to obtaining details of the person's "village, traditional authority and district of origin"[24], "postal address, e-mail address and telephone contacts"[25], implying that where such details are not applicable, they are not required. There are people in Malawi who have lived their lives in a town (they do not have a home village), and this allows for flexibility in the application of the CDD requirements.

The CDD requirements contained in the abovementioned regulations represent a robust understanding of the local circumstances. They have been drafted, taking into account ML/TF risk. The study conducted is not designed to reflect on the effectiveness of the respective regulatory requirements, however, the approach adopted is needed to address financial exclusion risk.

Regulation 10 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 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 line with the requirements of FATF Recommendation 10, Regulation 22 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to conduct ongoing due diligence on their customers, and to develop risk-based systems and procedures for this purpose.[26] In addition, reasonable steps must be taken to ascertain the purpose of any transaction, including deposits, in excess of K1, 000,000, as well as the origin of such funds and their ultimate destination.[27]

[23] This statement was made by the FIU in a meeting held in Malawi in May 2013.
[24] Regulation 4(1)(d) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.
[25] Regulation 4(1)(e).
[26] Regulation 22(1).
[27] Regulation 22(2). In terms of Regulation 22(4), financial institutions are required to have automated or manual systems that trigger action in the event that all thresholds referred to in the regulations are exceeded.

3.3 Timing of verification of identity

Section 24 (1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[28] requires a financial institution to verify a customer's identification or beneficial owner on the basis of reliable and independent source documents "before entering a business relationship". In this regard, a business relationship is defined to include an occasional transaction. Section 25 (1) specifically prohibits a financial institution from proceeding with any transaction in the absence of satisfactory identification, unless directed to do so by the FIU.[29]

Regulation 9(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires a financial institution to verify the identity of a customer or beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Financial institutions are also required to keep evidence of the original identification document. Financial institutions may in specific circumstances defer verification.

The Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[30] does not contain any provisions requiring financial institutions to terminate business relationships, in the event that satisfactory customer identification information is not obtained by the financial institution. This matter is however covered by Regulation 3(9) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 which reads, "where a financial institution has failed to obtain satisfactory evidence of the identity of a customer in accordance with regulations 3 to 8, it shall (a) not open the account, commence business relationship or perform a transaction unless advised otherwise by the FIU; (b) suspend or close the account unless advised otherwise by the FIU; and (c) submit a suspicious transaction report in respect of the attempted transaction."

3.4 Risk-based approach to CDD: Simplified Measures

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) Customers whose average monthly income does not exceed K50,000; and
(d) Other forms of low risk categories of customers, beneficial owners, beneficiaries or business relationships.[31]

From a financial inclusion perspective, it is encouraging to see that low income customers are specifically mentioned together with other low risk categories of customers, beneficial owners, beneficiaries or business relationships. The Regulation does not however refer to low risk products

[28] Act 11 of 2006.
[29] Failure to abide by this prohibition of Section 25 (1) subjects natural persons to two years imprisonment and a K100, 000 fine and corporates to a K500,000 fine and the loss of their business license.
[30] Act 11 of 2006.
[31] 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."

with specific requirements and limits, although upon a broad interpretation of the wording, this is inferred.

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 contrasts 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."[32]

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

Record keeping requirements are set out in section 27 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[33] and Regulation 17 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.

Financial institutions are required to establish and maintain records of –

(a) The identity of a person;
(b) All transactions carried out and correspondence relating to transactions as is necessary to enable a transaction to be readily reconstructed at any time by the Financial Intelligence Unit or competent authority[34];
(c) All reports made to the Financial Intelligence Unit; and
(d) Enquiries relating to money laundering and financing of terrorism made to it by the Financial Intelligence Unit.[35]

The records must be kept for a minimum period of seven years from the date (a) the evidence of a person's identify was obtained, (b) of any transaction or correspondence, (c) the account is closed or business relationship ceases, whichever is the latter.[36] This is over and above the five years required by FATF Recommendation 11.

Section 27(4) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 requires that a copy of the record, together with the appropriate back–up and recovery procedures, be kept in a manner as the Minister may prescribe by regulation.

---

[32] Section 100(1) reads "A financial institution in Malawi shall (a) demand proof of and record the identities of its clients or customers, whether usual or occasional when establishing business relations or conducting occasional transactions and in particular when performing large cash transactions."
[33] Act 11 of 2006.
[34] These must contain the particulars as the Minister may prescribe by regulation.
[35] Section 27(1) Act 11 of 2006.
[36] Section 27(2).

Regulation 17 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 reads:

"17(1) A financial institution shall keep all records in soft and hard copy form, and it shall ensure that appropriate backup and recovery procedures are in place.

(2) A financial institution shall take reasonable steps, in respect of an existing business relationship, to maintain the correctness of records in compliance with regulations 4 to 15 by undertaking a two-year review of existing records, particularity for higher risk categories of customers and business relationships."

FATF Recommendation 11 does not specifically require that a photocopy (hard copy) of the identification documents presented for verification purposes be kept. (It merely requires that the information on that document be stored and kept for five years.) The need to store a physical copy of documents obtained places a burden on financial institutions (compliance with Regulation 17(1)) and adversely impacts access to financial services. It is understood that, at this juncture, regulators expect institutions to keep hard copy records as a result of identified record keeping challenges, i.e. in the absence of sound controls relating to electronic records.

As per section 27(5) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006, records maintained must be made available upon request to the Financial Intelligence Unit or other competent authority for the purpose of ensuring compliance with the Act, and for the purpose of the investigation and prosecution of an offence.

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

Section 24(4), section 24(6) and section 24(7) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and Regulation 19 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 deal with correspondent banking. In terms of section 24(4), every financial institution is required in relation to its cross–border correspondent banking and other similar relationships to adequately identify and verify the respondent institution with which it conducts such a business relationship; gather sufficient information about the nature of the business of the correspondent institution, determine from publicly available information the reputation of the person and the quality of supervision to which the correspondent institution is subject, assess the anti-money laundering and terrorist financing controls of the correspondent institution, obtain approval from senior management before establishing a new correspondent relationship and document the responsibilities of the financial institution and the correspondent institution.

Regulation 19(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 contains comprehensive provisions in relation to correspondent banking and other similar business relationships. This occurs specifically where financial institutions are required to adequately identify and verify the correspondent institution or a respondent institution, whichever is applicable[37], and to gather sufficient information about the nature of the business of the correspondent institution or respondent institution.[38] From publically available information, financial institutions are required to determine the reputation of the institution and the quality of

[37] Regulation 19(1)(a) of Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.
[38] Regulation 19(1)(b).

supervision to which the correspondent or a respondent institution is subjected.[39] In addition, financial institutions are required to 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[40], obtain approval from senior management before establishing a new correspondent or a respondent relationship[41], obtain documents or agreements signed by senior management of the correspondent and a respondent institution of the respective responsibilities of each institution[42], and obtain certification from the correspondent or a respondent institution certifying that in line with regulation 21(1), it carries out due diligence on other correspondent or respondent institutions which provide similar services and (ii) the correspondent or a respondent institution does not provide similar services to shell banks.[43]

Regulation 19(3) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 specifically states that "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."

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

Money value transmitters that handle foreign currency are licensed under the Exchange Control Act, 1989 as foreign exchange dealers. Every financial institution licensed under the Banking Act requires a separate license under the Exchange Control Act in order to deal in foreign currency.[44] The Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[45] also designates "any person who conducts business performing money transmission services" as a financial institution and as such, are subject to the provisions of the Act. In terms of section 33(1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006, every institution or person that is licensed to do business in Malawi as a financial institution under the Banking Act, or a money transmission service, is required to include accurate originator information and other related messages with electronic funds transfers, and this information is required to remain with the transfer.[46]

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

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

[39] Regulation 19(1)(c).
[40] Regulation 19(1)(d).
[41] Regulation 19(1)(e).
[42] Regulation 19(1)(f).
[43] Regulation 19(1)(g).
[44] 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 Malawi.*
[45] Act 11 of 2006.
[46] As per section 33(2)(a) and (b), this does not apply to "electronic funds transfer, other than a money transfer effected from the use of a credit or debit card as a means of payment that results from a transaction carried out using a credit or debit card. Provided that the credit or debit card number is included in the information accompanying such a transfer, and (b) electronic funds transfer and settlements between financial institutions where the originator and beneficiary of the funds transfer are acting on their own behalf."

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.

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

Section 33 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[47] is applicable to wire transfers and states simply that, "every institution or person that is licensed to do business in Malawi as a financial institution under the Banking Act or a money transmission service provider shall include accurate originator information and other related messages on electronic funds transfers, and such information shall remain with the transfer."

Malawi, like Lesotho, refers to "electronic funds transfers" instead of "wire transfers" in Regulation 18 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011. In terms of this Regulation, a financial institution is required to meet exchange control requirements to transfer money, which include: (a) accurate originator information (name of originator, address of the originator, an account number of the originator and other related messages that are sent); and (b) accurate beneficiary information (name of beneficiary, address of the beneficiary, an account number of the beneficiary, SWIFT code and other related messages that are sent). The information is required to remain with the fund transfer or related message through the payment chain.[48] Financial institutions are also required to verify the identity of the originator and beneficiary[49], and ensure that an intermediary institution in the payment chain provides all originator information and beneficiary information which must also accompany an electronic funds transfer.[50] In addition, financial institutions are required to monitor and report to the FIU suspicious electronic funds transfers which do not contain complete originator and beneficiary information and restrict or terminate a business relationship with a financial institution which persistently fails to include originator information in its electronic funds transfers.[51]

Neither the law nor regulations contain the suggested *de minimus* threshold of US$1,000.

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

Section 24 (6) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[52] provides a reasonably comprehensive set of requirements for introduced business .[53] In addition, the use of third parties is covered by Regulation 20(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 that requires financial institutions which choose to rely on an intermediary or third party to undertake their obligations under Parts II and III of the regulations or to introduce business to enter into an agreement with the third party outlining the roles and responsibilities of each party. Financial institutions are also required to immediately

[47] Act 11 of 2006.
[48] Regulation 19(1)(a) and 19(1)(b) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.
[49] Regulation 19(2).
[50] Regulation 19(3).
[51] Regulations 19(4) and 19(5).
[52] Act 11 of 2006.
[53] 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 Malawi.

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.[54] 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 set out in the Act.[55] Section 21(1)(f) of Malawi's Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[56] specifically states that "financial institutions which rely on third parties or intermediaries shall ultimately be responsible for customer identification and verification."

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

The internal controls requirement is covered by section 32 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006, but the Act does not cover the issue of foreign branches. Foreign branches and subsidiaries are however covered by Regulation 28 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 which requires financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and the regulations.[57] If the minimum requirements of the host country are lower than the requirements applicable in Malawi, financial institutions are required to ensure that their branches and subsidiaries apply the higher standards.[58] Regulation 28(3) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to inform the FIU and Supervisory Authorities if their foreign branch or subsidiary is unable to observe appropriate AML/CFT measures.

Section 32 (1) (b) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[59] requires each financial institution to establish procedures and systems that address customer identification, record keeping, detection of suspicious transactions and the reporting of such transactions, and make the institution's officers and employees aware of laws and regulations concerning money laundering and the financing of terrorism, as well as the institution's own policies and procedures regarding these requirements.

Section 32 (1) (a) and 32 (2) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 require the appointment of a Compliance Officer to be a senior officer and specifies the duties of such an officer, including the responsibility for developing a compliance manual for the institution. The requirement of the appointment of a Compliance Officer does not apply to institutions with five or less employees. Additional responsibilities of the Compliance Officer are set out in Regulation 27. Specifically, Regulation 27(1)(b) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires the Compliance Officer to apply internal risk management procedures to suspicious transactions disclosures from officers and employees of the financial institution, and report disclosures deemed suspicious to the FIU.

[54] Sections 24(6)(a) and (b).
[55] Section 24(6)(c).
[56] Act 11 of 2006.
[57] Regulation 28(1) Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.
[58] Regulation 28(2).
[59] Act 11 of 2006.

Regulation 16(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 requires financial institutions to develop and update on a regular basis a written risk-based Customer Acceptance Policy for both ongoing business and single transactions. The Regulation also requires financial institutions to have procedures and guidelines explaining the Customer Acceptance Policy. These procedures and guidelines must form part of the institution's training programmes.

The Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and the Regulations do not address the requirement that financial groups should have group-wide AML/CFT programmes that include policies on information sharing within the group.

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

Section 28(1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 requires that "whenever a financial institution processes a transaction exceeding such amount of currency or its equivalent in foreign currency... [as prescribed by the Minister], or suspects or has reasonable grounds to suspect that any transaction is related to the commission of a money laundering offence or terrorist financing, it shall as soon as possible - but not later than three working days after forming that suspicion - report it in writing to the FIU. 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, 2006, shall report such a 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 the FIU electronically in an encrypted format no later than three days after the suspicion is formed. All reporting institutions are required to report to the FIU on a weekly basis in respect of the Large Currency Transaction report that must be submitted.[60]

As per section 28(1) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[61], financial institutions are also required to report large transactions exceeding such amount of currency or its equivalent in foreign currency as the Minister may, from time to time, prescribe by notice published in the Gazette. This threshold is currently set at 1,000,000.00 Malawian Kwacha that is equivalent to US$ 2,284.98.[62] Analysts at the FIU receive these reports and undertake the required analysis relating thereto. If a suspicious transaction is found, the FIU hands it over to the relevant authority (Anti-Corruption Bureau, Revenue Authority, National Intelligence Bureau, etc.) for investigation.

[60] Regulation 25 reads "In accordance with section 28 of the Act, a financial institution shall submit the following reports to the FIU – (a) a Weekly Transaction Report in a format specified in the First Schedule; or (b) a Large Currency Transaction Report (LCTR) in a format specified in the Second Schedule."

[61] Act 11 of 2006.

[62] Exchange rate as of 31/03/2015. (This threshold seems very low and places quite a large burden on accountable institutions and the FIU). Such reporting may not be sustainable in the long run.

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

Regulation 29(1) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 states that the FIU may, from time to time, issue and revise existing guidelines for the operation of the Act and these Regulations. The guidelines may prescribe particulars or matters, including forms, deemed necessary or expedient for the operation, or use in operation of the Regulations. To date, no guidelines have been issued by the FIU. In addition, it is noted in the Mutual Evaluation report that "the FIU has not provided any feedback to reporting institutions, other than acknowledgement of the receipt of reports." At the time of the mutual evaluation this was 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 acknowledgements." [63] The FIU has indicated that banks are now provided with "sanitised cases" every fortnight as feedback and that it meets with compliance officers every quarter to provide feedback / guidance. The FIU also provides reporting trends so that each bank understands how well they are doing in terms in of the relevant report requirements.

13. High Level Recommendations for Malawi

The recommendations set out in Table 3 below are not intended to be exhaustive. These high level recommendations provide an indication on how specific sections in the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[64] and Regulation in the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 could be amended to bring the law in line with the several of the revised FATF Recommendations.

Table 3: High Level Recommendations for Malawi

R10	CDD: Component A - When CDD is Required
It is recommended that consideration should be given to increasing the threshold specified in Regulation 3(1)(c) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 – i.e. from K500,000 which is equivalent to USD1142.49 to an acceptable level that is commensurate with the risks identified in the Malawian context. It is understood that, at this juncture, regulators expect institutions to keep hard copy records as a result of identified record keeping challenges, i.e. in the absence of sound controls relating to electronic records. However, it is noted that, over time, as technology driven delivery channels develop, there will be opportunities to develop technology-enabled CDD. This will provide a platform for increased access to financial services.	
R10	CDD: Component B - Identification Measures and Verification Sources
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. Regulation 10, which deals with the verification of details required in regulation 4(1) and 4(2), makes	

[63] 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 Malawi.*
[64] Act 11 of 2006.

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. This approach should be encouraged in the other SADC countries.

R10	CDD: Component C - The Timing and Verification of Identity

Compliant with Component C of Recommendation 10.

R10	CDD: The Risk-Based Approach to CDD - Simplified Measures and Exemptions

Regulation 3(5) 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) 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.[65] From a financial inclusion perspective it is encouraging to see that low income customers are specifically mentioned together with other low risk categories of customers, beneficial owners, beneficiaries or business relationships. The Regulation does not however refer to low risk products with specific requirements and limits, although upon a broad interpretation of the wording, this is inferred.

It is recommended that simplified due diligence procedures be specifically mandated for specified (banking) 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 and the Proven Low Risk Exemption for Low Value Prepaid Instruments.)

R11	Record Keeping

As FATF Recommendation 11 does not specifically require that a photocopy (hard copy) of the identification documents presented for verification purposes be kept (it merely requires that the information on that document be stored and kept for five years), it is unclear why there is a need to store a physical copy and an electronic copy which makes compliance with Regulation 17(1) an unnecessary burden on financial institutions. It is submitted that, where institutions have adequate electronic version controls, this could promote access to financial services going forward.

It is also recommended that Malawi consider the regulatory record keeping burden relating to the seven year record keeping period (particularly where this will adversly impact on financial inclusion), i.e. in the light of the five year period as suggested by FATF. This will ease the regulatory compliance burden substantially and harmonise domestic requirements with those applied by the majority of SADC countries that mandate the five year timeframe.

[65] 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."

R13	Correspondent Banking
Section 24(4), section 24(6) and section 24(7) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[66] and Regulation 19 of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011 deal with correspondent banking and are compliant with FATF Recommendation 13.	
R15	New Technologies
Regulation 23 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" may 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. It is recommended that these deficiencies be addressed as soon as is reasonably practicable.	
R16	Wire Transfers
Section 33 of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 is applicable to wire transfers. In addition, Malawi refers to "electronic funds transfers" instead of "wire transfers" in Regulation 18. Both section 33 and Regulation 18 are 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.[67]	
R17	Reliance on Third Parties
Section 24 (6) of the Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006[68] provides a reasonably comprehensive set of requirements for introduced business. In addition, the use of third parties is covered by Regulation 20(1) and requires financial institutions which choose to rely on an intermediary or third party to undertake their obligations under Parts II and III of the regulations or to introduce business to enter into an agreement with the third party outlining the roles and responsibilities of each party. These provisions are compliant with FATF Recommendation 17.	
R18	Internal Controls
The Money Laundering Proceeds of Serious Crime and Terrorist Financing Act, 2006 and the Regulations do not address the new FATF requirement that financial groups should have group-wide AML/CFT programmes that include policies on information sharing within the group. It is recommended that this deficiency be addressed as soon as is reasonably practicable. It is understood that this is being addressed in revised regulatory requirements.	

[66] Act 11 of 2006.
[67] Interpretive Note to Recommendation 16, paragraph 5.
[68] Act 11 of 2006.