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

Swaziland Country Report

Finalised by: Compliance & Risk Resources

March 2015

Contents

SWAZILAND 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 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 Post February 2010

The Eastern and Southern Africa 'Anti-Money' Laundering Group (ESAAMLG) Mutual Evaluation report for Swaziland was adopted in September 2012 and published in November 2012.[1].

The evaluation made extensive use of the old Anti-Money Laundering Act, the Money Laundering (Prevention) Act, 2001[2], which has subsequently been repealed by the enactment of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. At the time of the in-country assessment, the Securities Act, 2010[3] was still a Bill.

In 2011, the National Clearing and Settlements System Act of 2011[4] was passed in 2011. The Minimum Standards for Electronic Payment Schemes, 2010 were issued by the Central Bank of Swaziland before the enactment of the National Clearing and Settlements System Act of 2011 under the powers conferred to it by sections 4 (f) and 42 (b) of The Central Bank of Swaziland Order 1974 (as amended). These Minimum Standards set out the Bank's position with respect to e-money (paragraph 3.0), and provide comprehensive Risk Management Standards (paragraphs 8 to 11).

Anti-Money Laundering and Counter-terrorist Financing (AML/CFT) Guidelines for Insurers and Intermediaries were issued by the Office of the Registrar of Insurance and Retirement funds (RIRF), in 2010.[5] These were revised in 2011.

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

Year	Legislation and Regulation Enacted and Issued Post ESAAMLG Evaluation
In-country Assessment February 2010 and February 2011 **Adopted** September 2012	• Securities Act 9 of 2010 • Minimum Standards for Electronic Payment Schemes, 2010 • The Money Laundering and Financing of Terrorism (Prevention) Act, 2011 • The National Clearing and Settlements System Act 17 of 2011 • Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guideline (Insurers and Intermediaries), 2010 (revised 2011)

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

Table 2 below provides an overview of the current laws, regulations, exemptions, guidelines and guidance notes in force in Swaziland 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 legislation in force in Swaziland is the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. No regulations have been issued pursuant to section 92 of the Act, however two sets of guidelines have

[1] *See Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)* 2010 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Kingdom of Swaziland.*
[2] Act 12 of 2001 (repealed).
[3] Act 9 of 2010.
[4] Act 17 of 2011.
[5] Issued pursuant to the old Money Laundering (Prevention) Act 12 of 2001.

been issued[6]. Swaziland also has a standalone counter terrorism Act, the Suppression of Terrorism Act, 2008 which commenced on the 21st September, 2008.

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

	Core Acts			Issued Under the Act
✓	Money Laundering and Financing of Terrorism (Prevention) Act 2011		✓	• Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines (Insurers and Intermediaries) 2010 • Anti-Money Laundering Guidelines 2011
✓	Suppression of Terrorism Act 2008		✗	
	Additional Relevant Legislation			
✓	Prevention of Corruption Act 2006		✗	
✓	Serious Offences (Confiscation of Proceeds) Act 8 of 2001		✗	
✓	Criminal Procedure and Evidence (Amendment) Act 67 of 1938 (As Amended)		✗	
✓	Customs and Excise Act 1971		✗	
✓	Exchange Control Order 1974		✗	
✓	Companies Act 8 2009		✗	
✓	Criminal Matters (Mutual Assistance Act) 2001		✗	
✓	Extradition Act 1968			
✓	Transfer of Convicted Offenders Act 2001			
✓	Fugitive Offenders Act 1969			
✓	Electronic Records (Evidence) Act 2009			
	Legislation Applicable to Banks			
✓	Central Bank of Swaziland Order 1974 Central Bank of Swaziland (Amendment) Act 1 2004		✓	• Minimum Standards for Electronic Payment Schemes, 2010
✓	Financial Institutions Act 6 2005			
✓	Financial Institutions Act 6 2005			
✓	National Clearing and Settlement Systems Act 17 of 2011			
	Legislation Applicable to NBFIs			
✓	Insurance Act 7 2005		✗	
✓	Securities Act 9 2010		✗	
✓	Retirement Funds Act 7 2005		✗	
	Legislation Applicable to DNBPs and NPOs			
✓	Casinos	Casino Act 53 1963 Lotteries Act 1963 Bookmakers Act 1970	✗	
✓	Lawyers	Legal Practitioners Act 1964 The Law Society of Swaziland Bye-Laws 1992	✓	• Legal Practitioners (Disciplinary Proceedings) Regulations 1989
✓	Accountants	Accountants Act 1985	✗	
✗	Precious Metals and Stones Dealers		✗	
✗	Estate Agents		✗	

[6] Section 92 of the Act reads, "The Minister may make regulations consistent with this Act- (a) for or with respect to any matter that by this Act is required or permitted to be prescribed; or, (b) that is necessary or convenient to be prescribed for carrying out or giving effect to this Act."

✘	NPOs			✘	

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

CDD requirements are found in sections 6 and 7 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011. Sections 9 and 73 cover the prohibition against opening, operating or maintaining any anonymous account or any account which is in a fictitious, false or incorrect name.

3.1 When is CDD required in Swaziland?

Accountable institutions listed in section 2 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 are, in compliance with section 6, required to undertake CDD measures.[7] Accountable institutions are required to ascertain the identity of a customer or beneficial owner before entering into a business relationship.[8] Accountable institutions must also verify identity when entering into a continuing business relationship,[9] conducting any transaction,[10] carrying out

[7] "An accountable institution means any person, including, but not limited to, a financial institution licensed under the Financial Institutions Act, 2005, who carries on the business or activity of: (a) acceptance of deposits and other repayable funds from the public, lending, including consumer credit, mortgage credit, factoring (with or without recourse) and financing of commercial transactions; (b) financial leasing; (c) money transmission services; (d) issuing and administering means of payment (such as credit cards, travelers' cheques and bankers' drafts); (e) financial guarantees and commitments; (f) trading for that person's own account or for the account of that person's customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate and index instruments, commodity futures trading and transferable securities; (g) participation in securities issues and the provision of services related to such issues; (h) money-broking; (i) individual and collective investment schemes or trustees of collective investment schemes; (j) safekeeping and administration of cash or liquid securities on behalf of other persons; (k) safe custody services; (l) investing, administering or managing funds or money on behalf of other persons; (m) an insurer, an insurance broker or an insurance underwriter; (n) trustee administrator or investment manager of a retirement scheme but excluding closed-ended schemes; (o) bureaux de change or foreign exchange dealer; (p) operating a gambling house, casino or lottery, including an operator who carries on such operations through the internet; (q) a trust or company service provider, not otherwise covered by this section, which as a business, provides, to third parties, the services of- (i) acting as a formation agent of legal persons; (ii) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; (iii) providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; (iv) acting as, or arranging for another person to act as, a trustee of an express trust; or (v) acting as, or arranging for another person to act as, a nominee shareholder for another person; (r) an offshore entity; (s) a lawyer, notary, conveyancer, other independent legal professional, or an accountant when preparing or carrying out transactions for a client concerning the following activities- (i) buying and selling of immovable property; (ii) managing of client money or trust funds, securities or other assets; (iii) management of bank, savings or securities accounts; (iv) organisation of contributions for the creation, operation or management of companies; or (v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities, (t) dealing in immovable property when the persons dealing are involved in transactions for their client concerning the buying and selling of real estate; (u) dealing in precious metals or stones, when the persons dealing engage in any cash transaction with a customer equal to or above the applicable designated threshold; or, (v) such other business as the Minister may, by Notice published in the Gazette, prescribe."

[8] Section 6(1) Money Laundering and Financing of Terrorism (Prevention) Act 2011.

[9] Section 6(1)(a)(i).

an electronic funds transfer,[11] where there is a suspicion of a money laundering offence or the financing of terrorism[12], or when the accountable institution has doubts about the veracity or adequacy of the customer identification and verification documentation or information it had previously obtained.[13]

Section 6(3) requires accountable institutions to take reasonable measures to ascertain the purpose of any transaction in excess of twenty thousand Emalangeni (E20, 000), or of ten thousand Emalangeni (E10, 000) in the case of cash transactions, and the origin and ultimate destination of the funds involved in the transaction. E20, 000 is equivalent to USD 1655.63and E10, 000 to USD 827.81. These amounts are below the FATF recommended threshold.

Section 7 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 contains two exemptions. CDD measures listed in sections 6(1), 6(2) and 6(3) do not apply in the following circumstances:

- If the transaction is part of an existing and regular business relationship with a person who has already produced satisfactory evidence of identity, unless the accountable institution has reason to suspect that the transaction is suspicious or unusual; or

- If the transaction is an occasional transaction not exceeding two thousand, five hundred Emalangeni (E2,500), unless the accountable institution has reason to suspect that the transaction is suspicious or unusual.

The latter exemption is a "Proven Low Risk Exemption" and could be argued to support a financial inclusion agenda. The amount is however extremely low (equivalent to USD 239.01), USD14760.99 below the Financial Action Task Force (FATF) recommendation of USD 15, 000. It is understood that the application of the exemption is limited as Swaziland has not yet undertaken a national risk assessment on Money Laundering and Terrorist Financing Risk.

In addition, the Central Bank of Swaziland has, through the Exchange Control Division, issued KYC Circular 1/2013 where verification for accounts with turnovers of E5000 or less will not require proof of residence, but only documentation to verify identity. This exemption is designed to support financial inclusion.

Section 9 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires accountable institutions to maintain accounts in the true name of the account holder.[14] Accountable institutions are thus prohibited from opening, operating or maintaining any anonymous account or any account which is in a fictitious, false or incorrect name.[15] Section 73 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 deals with the situation where a person is commonly known by two or more different names and specifically prohibits a person from using one of those names in opening an account with a reporting entity, unless the person has previously disclosed the other name or names to the reporting entity. Section 73(2) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 also requires the accountable institution, where a person using a particular name in his or her dealings with an accountable institution discloses to it a different name or names by which he or she is commonly

[10] Section 6(1)(a)(ii).
[11] Section 6(1)(b).
[12] Section 6(1)(c).
[13] Section 6(1)(d).
[14] Section 9(1).
[15] Section 9(2).

known, to make a record of the disclosure and, at the request of the Swaziland Financial Investigation Unit (SFIU), give the SFIU, a copy of the record.

3.2 Identification measures and verification sources

For transactions conducted by natural persons, accountable institutions are required to adequately identify and verify the identity of the person and acquire:

- The name, physical address and occupation of the person; and
- The national identity card or passport or other applicable official identifying document.[16]

No regulations have been issued on how to verify a person's address or what would constitute "other applicable official identifying document". The Central Bank of Swaziland has set up an AML Working Group with the compliance officers of accountable institutions to discuss matters of compliance, including identifying documents acceptable for verification of a person's address and suitable alternatives in circumstances where they are unable to verify such an address.

Section 6(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires that identification be done on the basis of any official identifying document and verification of 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."

Section 6(2)(a) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires accountable institutions, when establishing a business relationship, to obtain information on the purpose and nature of the business relationship. Section 6(2)(b) also requires accountable institutions to take reasonable measures to establish the source of wealth and property of a person.

In terms of section 6(2)(c) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011, if the transaction is conducted by a legal entity, accountable institutions are required to adequately identify and verify its legal existence and structure, including information relating to:

- The customer's name, legal form, address and directors;
- The principal owners and beneficiaries and control structure; and
- The 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.[17]

Section 6(8) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 specifically states that the Minister may, by Notice published in the Gazette, prescribe the official or identifying documents, or the reliable and independent source documents, data or information or other evidence that is required for identification or verification of any particular customer or class of customers[18] or the threshold for, or the circumstances in which, certain provisions shall apply in relation to any particular customer or class of customers.[19] At the time of preparing this report, no such notices had been published.

[16] Section 6(2)(b).
[17] Section 6(2)(c).
[18] Section 6(8)(a).
[19] Section 6(8)(b).

Ongoing due diligence is provided for in section 11(3) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 which reads, "an accountable institution shall monitor its business relationships and the transactions undertaken throughout the course of the relationship to ensure that its obligations under section 6 are met, and that the transactions conducted are consistent with the information that the accountable institution has of its customer and the profile of the business of the customer."

3.3 Timing of verification of identity

As per the requirements set out in section 6(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011, accountable institutions are required to ascertain the identity of a customer or beneficial owner before entering into a business relationship and conducting any transaction.

If satisfactory evidence of the identity of a customer is not produced or obtained by an accountable institution in accordance with section 6 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011, the accountable institution is required to report the attempted transaction to the SFIU and is prohibited from undertaking further transactions unless directed to do so by the SFIU.[20]

The Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not contain any provisions permitting accountable institutions to complete the verification process as soon as reasonably practicable following the establishment of a business relationship where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

3.4 Risk-based approach to CDD: Simplified Measures

Other than the low risk exemptions set out in Section 7 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011, as discussed earlier in this report, the Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not contain any further provisions allowing for simplified CDD measures. A law review committee has been established to address these shortcomings.

It was noted in the Save the Children report entitled *Distributing Cash through Bank Accounts – Save the Children's Drought Response in Swaziland* that the Central Bank of Swaziland are open to reducing the Know Your Customer (KYC) requirements for specific products that provide appropriately defined and limited services for specific types of customers, in this case, recipients of an emergency cash transfer.

"Save the Children used its field workers to ensure that all recipients had the necessary documentation and completed forms to open the accounts. Standard Bank then verified each application for KYC requirements. To facilitate the account opening process, the bank had negotiated with the Central Bank of Swaziland that certain KYC requirements be relaxed for these accounts. This meant that instead of having to produce a utility bill as proof of residence, the

[20] Section 7.

beneficiaries could get a letter from their chief certifying that they lived in his chiefdom. They also had to have ID cards."[21]

The Central Bank of Swaziland has, through the Exchange Control Division, issued KYC Circular 1/2013 where verification for accounts with turnovers of E5000 or less will not require proof of residence, but only documentation to verify identity. This exemption is designed to support financial inclusion.

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

Section 8(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires accountable institutions to establish and maintain records of the identity of a person obtained in accordance with section 6, all transactions carried out by it and correspondence relating to the transactions as is necessary to enable the transaction to be readily reconstructed at any time by the SFIU or competent authority, all reports made to the SFIU under section 12, and all enquiries relating to money laundering and financing of terrorism made to it by the SFIU. Records must be kept for a minimum period of five years.[22] The Act is not specific about the manner in which the records are to be kept, save to say, that "where any record is required to be kept under this Act, a copy of it, with the appropriate back-up and recovery procedures, shall be kept in a manner as the Minister may by Regulation prescribe."[23] Swaziland has passed the Electronic Records (Evidence) Act, 2009, which prescribes how records should be kept in order for them to be admissible in a Court of Law.

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

Correspondent Banking is covered in section 6(4) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011. Accountable institutions are required, in relation to their cross-border correspondent banking and other similar relationships, to:

- Adequately identify and verify the respondent institution with which it conducts such a business relationship[24];
- Gather sufficient information about the nature of the business of the respondent institution[25];
- Determine from publicly available information the reputation of the person and the quality of supervision to which the respondent institution is subject[26];
- Assess the respondent institution's anti-money laundering and terrorist financing controls[27]; and

---

[21] Beswick C *Distributing Cash Through Bank Accounts Save the Children's Drought Response in Swaziland* 17.

[22] Section 8(2) states further that records must be maintained for five years from the date (a) the evidence of the identity of a person was obtained; (b) of any transaction or correspondence; (c) the account is closed or business relationship ceases, whichever is the later.

[23] Section 8(4) Money Laundering and Financing of Terrorism (Prevention) Act 2011.

[24] Section 6(4)(a).

[25] Section 6(4)(b).

[26] Section 6(4)(c).

[27] Section 6(4)(d).

- Obtain approval from senior management before establishing a new correspondent relationship[28] and document the responsibilities of the accountable institution and the respondent institution.[29]

In circumstances where the relationship is a payable-through account, accountable institutions are required to ensure that the institution with whom they have established the relationship has verified the identity of and performed on-going due diligence on such of the customers of that institution that have direct access to accounts of the accountable institution and, are able to provide the relevant customer identification data upon request.[30]

Whilst mostly compliant with FATF Recommendation 13, the Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not contain any provisions prohibiting financial institutions from entering into, or continuing correspondent banking relationships with shell banks or to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

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

Banks and the Post Office money, or value transfer services, are licensed by the Central Bank of Swaziland. As part of its normal business operations, Banks are allowed to carry on money or value transfer services for occasional and regular clients. The Post Office operates money transmission orders. As noted by ESAAMLG, "although there is no direct legal prohibition, independent money or value transfer, operators are not licensed in the country. Independent MVT operators can only operate money or value transfer through a principal-agent business arrangement, whereby an MVT operator is allowed to use its money or value transmission technology to provide MVT services as part of business operations of a licensed bank in the Kingdom of Swaziland. Only Money Gram operated under this arrangement."[31]

Section 10(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 applies both to financial institutions and money transmission service providers, and requires these accountable institutions to include accurate originator information and other related messages with electronic funds transfers, and such information shall remain with the transfer. Section 10(2) reads "subsection (1) shall not apply to an electronic funds transfer, other than a money transfer effected from the use of a credit or debit card as means of payment that results from a transaction carried out using a credit or debit card, where the credit or debit card number is included in the information accompanying such a transfer." The information required for CDD would, in that instance, already be held by the accountable institution that issued the credit or debit card, and the details of the account holder can be traced through the account number.

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

The Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not contain any provisions requiring accountable institutions to identify and assess the money laundering or

[28] Section 6(4)(e).
[29] Section 6(4)(f).
[30] Section 6(5)(a) and (b).
[31] *Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)* 2010 *Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism: Kingdom of Swaziland* 141.

terrorist financing risks that may arise in relation to the development of new products, business practices and delivery mechanisms, or the risks that may arise through the use of new or developing technologies. The Minimum Standards for Electronic Payment Schemes, issued by the Central Bank of Swaziland in 2010 pursuant to the powers conferred to it by sections 4 (f) and 42 (b) of The Central Bank of Swaziland Order 1974 (as amended), do not contain any AML/CFT-related provisions.

The Central Bank of Swaziland has issued Guidelines for Mobile Payments.[32] During a meeting with the Central Bank of Swaziland, it was ascertained that these Guidelines had been used as the basis upon which to authorise MTN to partner with FNB in the roll-out of a mobile payment product in Swaziland.[33] The product known as *MTN Mobile Money* has much lower CDD requirements than a conventional bank account, and MTN agents are responsible for undertaking CDD and only require customers to produce an ID book and have a current mobile number. MTN Agents are supposed to take photostat copies of ID books and send these through to the MTN Head Office for record purposes. The Central Bank undertook an onsite inspection in July 2013, where it was noted that most MTN Agents do make copies of IDs and send them to MTN headquarters.[34] The product is subject to threshold limits, with the maximum amount set at E4 000 and the minimum at E20.

According to the Central bank of Swaziland, FNB has apparently expressed concerns regarding the fact that MTN are setting up kiosks throughout the country to offer these services and despite the fact that FNB is the prudentially regulated banking partner, their branding is conspicuous by its absence. It was also noted that FNB are not sure if MTN agents are depositing the required equivalent amount of real money into the FNB account before issuing "electronic money" to their customers. Several loopholes in the manner in which the system has been set up have already been established. For instance, under the Guidelines, each person is only allowed to have one mobile money account, but several people have been discovered to have two. This was achieved through using their ID book to open an account at one Agent, and their passport to open another account at a second agent.

Despite the fact that FNB holds the trust account for the mobile payments product and are the prudentially regulated financial institution, MTN are the partner required to submit returns to Bank Supervision. The Central Bank reported that FNB has nothing to do with the submission of these returns.

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

Section 10(1) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 applies both to financial institutions and money transmission service providers, and requires these accountable institutions to include accurate originator information and other related messages with electronic funds transfers, and such information shall remain with the transfer. This does not apply to electronic funds transfers and settlements between financial institutions where the originator and beneficiary of the funds transfers are acting on their own behalf.[35] As no regulations have been issued under the Money Laundering and Financing of Terrorism (Prevention) Act 2011, no details are provided with respect to the content of the "accurate originator information and other related

[32] We were however not provided with a copy of these Guidelines, and they are not publically available on the Internet.
[33] This meeting was conducted in Swaziland in March 2013.
[34] The Central Bank of Swaziland did however note that they had undertaken a spot check of a number of Agents, but were not forthcoming on the outcome of this exercise.
[35] Section 10(3) Money Laundering and Financing of Terrorism (Prevention) Act 2011.

messages". The provision does also not distinguish between the information required for domestic versus cross-border wire transfers.

Section 11(1)(d) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires accountable institutions to pay special attention to electronic funds transfers that do not contain complete originator information. Section 11 (2) (a) states that in relation to subsection (1), an accountable institution shall examine as far as possible the background and purpose of the transactions or business relations and record its finding in writing and (b) upon request, make available such findings to the SFIU or to competent authority, to assist the SFIU or the law enforcement agency in any investigation relating to an unlawful activity, a money laundering offence or an offence of financing terrorism.

The law does not contain the suggested *de minimus* threshold of US$1,000.[36]

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

Section 6(6) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 permits accountable institutions to rely on intermediary or third parties to undertake their obligations under subsections 6(1) and 6(2), or to introduce business. As is required by FATF Recommendation 17, accountable institutions are required to immediately obtain the information and documents required,[37] to ensure that copies of identification data and other relevant documentation relating to the requirements in the Act will be made available to them from the intermediary or the third party upon request without delay[38] and satisfy themselves that the third party or intermediary is regulated and supervised for, and has measures in place to comply with the requirements set out in sections 7, 8 and 9 of this Act.[39]

The Money Laundering and Financing of Terrorism (Prevention) Act 2011 does not contain any provisions related to reliance by a financial institution on a third party that is part of the same financial group.

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

Section 18 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 requires accountable institutions to appoint a Compliance Officer who shall be responsible for[40]:

- Ensuring the accountable institutions' compliance with the requirements of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 ;
- Establishing and maintaining procedures and systems to implement the customer identification requirements set out in section 6 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 ;
- Implementing record keeping and retention requirements under sections 8 and 9;

[36] Interpretive Note to Recommendation 16, paragraph 5.
[37] Section 6(6)(a) Money Laundering and Financing of Terrorism (Prevention) Act 2011.
[38] Section 6(6)(b).
[39] Section 6(6)(c).
[40] Section 18(2) requires that the compliance officer be a senior officer with relevant qualifications and experience to enable him or her to respond sufficiently well to enquiries relating to the accountable institution and the conduct of its business.

- Implementing the reporting requirements under section 12;
- Making its officers and employees aware of the laws and regulations relating to money laundering and financing of terrorism;
- Making its officers and employees aware of the procedures, policies and audit systems adopted by it to deter money laundering and financing of terrorism;
- Screening persons before hiring them as employees;
- Training its officers, employees and agents to recognise suspicious transactions, trends in money laundering and financing of terrorism activities and money laundering and financing of terrorism risks within accountable institutions' products, services and operations; and
- Establishing an audit function to test its anti-money laundering and financing of terrorism procedures and systems.[41]

An accountable institution that, in the course of carrying on its business, does not employ more than five persons, is exempt from appointing a Compliance Officer and establishing an audit function.[42]

The new FATF Recommendation 18 introduces the requirement that financial groups should have group-wide AML/CFT programmes that include information sharing within the group. This is not sufficiently covered in the Money Laundering and Financing of Terrorism (Prevention) Act 2011. Further, 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. This is also not covered in the Money Laundering and Financing of Terrorism (Prevention) Act 2011. In this regard, it is noted by ESAAMLG that, "this FATF Recommendation does not apply to the Kingdom of Swaziland since domestic financial institutions do not have foreign branches and subsidiaries operating in other jurisdiction(s)." It would however be wise to include such a provision in the Money Laundering and Financing of Terrorism (Prevention) Act 2011 in the event that one or more of Swaziland's accountable institutions (broader than banks), elects to expand their operations into other jurisdictions.

11. Swaziland's Approach to Recommendation 20: Suspicious Transaction Reports

In terms of section 19 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 , the Swaziland Financial Intelligence Unit (SFIU) has the specific mandate to receive STRs, analyse them and forward them to law enforcement.[43] The obligation for accountable institutions, the supervisory authority or an auditor of an accountable institution to report suspicious transactions are set out in section 12 and section 13 of the Act.[44] Accountable institutions are required to report the suspicious transaction or attempted transaction to the SFIU no later than two days after forming the suspicion.[45] The law specifically states that the report made shall be in writing and may be given by way of mail, telephone to be followed up in writing, fax or electronic mail, or such other manner as may be prescribed by the SFIU.[46] Several of the commercial banks interviewed during

[41] Section 18(1).
[42] Section 18(3).
[43] Section 19 reads "a financial intelligence unit to be known as the Swaziland Financial Intelligence Unit ("SFIU") is hereby established which shall be an autonomous central national agency responsible for receiving, requesting, analysing and disseminating to competent authorities disclosures of financial information as required under this Act in order to counter money laundering and financing of terrorism."
[44] Section 12 and s13.
[45] Section 12(1)(b)(ii).
[46] Section 12(2)(a).

March 2013 expressed the concern that section 12 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 is in conflict with the wording in section 38 of the Financial Institutions Act, 2005[47].This section reads:

"38 (1) No financial institution shall carry out a transaction which it knows or suspects to be related to a serious criminal activity until it reports the information regarding the transaction that indicates such activity to the Bank."

In 2012, during one of the meetings of the AML Working Group, where all Compliance Officers from the Commercial Banks and the Building Society are represented, this issue was tabled and it was agreed that the Money Laundering and Terrorism Financing (Prevention) Act, 2011 supersedes the FIA, 2005 when it comes to STR reporting. It was also agreed that Commercial Banks and Building Societies will have to make a business decision on whether to continue the relationship with a suspicious client or not.

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

Section 12(4) of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 is the only section in the Act that requires the SFIU to give feedback to accountable institutions. This feedback is only in the case where the SFIU has reasonable grounds to suspect that a transaction or a proposed transaction may involve an offence of financing of terrorism, the proceeds of an unlawful activity or a money laundering offence. Under these circumstances, the SFIU may direct the accountable institution in writing or by telephone, to be followed up in writing within one working day, not to proceed with the carrying out of that transaction or proposed transaction, or any other transaction in respect of the funds affected by that transaction or proposed transaction, for a period as may be determined by the SFIU. This may not be more than five working days, in order to allow the SFIU to make necessary inquiries concerning the transaction and, if the SFIU deems it appropriate, to inform and advise a competent authority.

The Act does not require the SFIU to provide feedback to accountable institutions under any other circumstances, although section 31 (h) requires the SFIU to compile statistics and records and disseminate information within Swaziland or elsewhere, as well as to make recommendations arising out of any information received and section 31(k) for the SFIU to provide training.[48] In Swaziland, it appears that the Supervisory Authorities are responsible for issuing guidelines to accountable institutions under their supervision. This reasoning is derived from the fact that section 31(i) states that "the SFIU is required to issue guidelines to accountable institutions **not under the jurisdiction of supervisory authorities** in relation to customer identification, record keeping and, reporting obligations and the identification of suspicious transactions."[49] To date, the CBS and the Office of the Registrar of Insurance and Retirement Funds have issued guidelines pursuant to the old Money Laundering (Prevention) Act 12/2001.The Anti-Money Laundering Guidelines (2001), issued by the CBS, are currently not being used in Swaziland and are currently being reviewed to bring them in line with the provisions of the new 2011 law.

[47] Act 6 of 2005.
[48] Section 31(k) reads, "the SFIU may provide training programmes for accountable institutions in relation to customer identification, record keeping and reporting obligations, and the identification of suspicious transactions."
[49] Section 31(i).

13. High Level Recommendations for Swaziland

The recommendations set out in Table 3 below are not intended to be exhaustive. These high level recommendations provide an indication on how sections in the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 could be amended to bring the law in line with the several of the revised FATF Recommendations.

Table 3: High Level Recommendations for Swaziland

R10	CDD: Component A - When CDD is Required
Section 6 of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 is largely compliant with FTAF Recommendation 10. However, section 6(1)(a)(ii) does not contain the suggested FATF threshold of USD15,000 and instead refers to "any transaction". Section 7 of the Money Laundering and Financing of Terrorism (Prevention) Act 2011 contains two exemptions. CDD measures listed in sections 6(1), 6(2) and 6(3) do not apply in the following circumstances: if the transaction is part of an existing and regular business relationship with a person who has already produced satisfactory evidence of identity, unless the accountable institution has reason to suspect that the transaction is suspicious or unusual; or, if the transaction is an occasional transaction not exceeding two thousand, five hundred Emalangeni (E2,500), unless the accountable institution has reason to suspect that the transaction is suspicious or unusual. The threshold of E2,500 for occasional transactions is extremely low (equivalent to USD 206.95), USD14, 757.21 below the FATF recommendation of USD 15, 000, and it is therefore recommended that the threshold be amended.	
R10	CDD: Component B - Identification Measures and Verification Sources
For transactions conducted by natural persons, accountable institutions are required to adequately identify and verify the identity of the person and acquire: • The name, physical address and occupation of the person; and, • The national identity card or passport or other applicable official identifying document. No regulations or guidelines have been issued on how to verify a person's address or what would constitute "other applicable official identifying document". Section 6(8) of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 specifically states that the Minister may, by Notice published in the Gazette, prescribe the official or identifying documents, or the reliable and independent source documents, data or information or other evidence that is required for identification or verification of any particular customer or class of customers[50] or the threshold for, or the circumstances in which, certain provisions shall apply in relation to any particular customer or class of customers.[51] At the time of preparing this report, no such notices had been published. This should be rectified as soon as is practicable.	
R10	CDD: Component C - The Timing and Verification of Identity
The Money Laundering and Financing of Terrorism (Prevention) Act, 2011 does not contain any provisions permitting accountable institutions to complete the verification process as soon as reasonably practicable following the establishment of a business relationship where the money laundering and terrorist financing risks are effectively managed, and where this is essential not to interrupt the normal conduct of business. It is recommended that the authorities consider remedying this omission as soon as is reasonably practicable.	

[50] Section 6(8)(a).
[51] Section 6(8)(b).

R10	CDD: The Risk-Based Approach to CDD - Simplified Measures and Exemptions
The Money Laundering and Financing of Terrorism (Prevention) Act, 2011 does not contain any provisions allowing for simplified CDD measures, nor does it mandate the application of a risk-based approach. It is recommended that Swaziland 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. The mandate to apply simplified due diligence measures should be specifically 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 and the Proven Low Risk Exemption for Low Value Prepaid Instruments.) Reporting entities should also be able to demonstrate to their supervisory authority that the extent of the measures is appropriate in relation to the risks of money laundering, financing of terrorism or other criminal conduct.	
R11	Record Keeping
The Money Laundering and Financing of Terrorism (Prevention) Act 2011 is not specific about the manner in which the records are to be kept, save to say, that "where any record is required to be kept under this Act, a copy of it, with the appropriate back-up and recovery procedures, shall be kept in a manner as the Minister may by Regulation prescribe." To date, no regulations have been issued. It is recommended that authorities consider issuing these regulations as soon as is reasonably practicable.	
R13	Correspondent Banking
Correspondent Banking is covered in section 6(4) of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 (MLFTPA). While mostly compliant with FATF Recommendation 13, the MLFTPA does not contain any provisions prohibiting financial institutions from entering into, or continuing correspondent banking relationships with shell banks, or to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks. It is recommended that the authorities consider resolving this deficiency as soon as is reasonably practicable.	
R15	New Technologies
The Money Laundering and Financing of Terrorism (Prevention) Act, 2011 does not contain any provisions requiring accountable institutions to identify and assess the money laundering or terrorist financing risks that may arise in relation to the development of new products, business practices and delivery mechanisms, or the risks that may arise through the use of new or developing technologies. The Minimum Standards for Electronic Payment Schemes, issued by the Central Bank of Swaziland in 2010 pursuant to the powers conferred to it by sections 4 (f) and 42 (b) of The Central Bank of Swaziland Order 1974 (as amended), do not contain any AML/CFT related provisions. It is recommended that that requirements relating to new technologies and non-face-to-face business are incorporated into the MLFTPA.	
R16	Wire Transfers
Section 10(1) of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 applies both to financial institutions and money transmission service providers, and requires these	

accountable institutions to include accurate originator information and other related messages with electronic funds transfers, and such information shall remain with the transfer. This does not apply to electronic funds transfers and settlements between financial institutions where the originator and beneficiary of the funds transfers are acting on their own behalf.[52] As no regulations have been issued under the Money Laundering and Financing of Terrorism (Prevention) Act 2011, no details are provided with respect to the content of the "accurate originator information and other related messages". The provision also does not distinguish between the information required for domestic versus cross-border wire transfers. It is recommended that authorities consider the inclusion of the suggested *de minimus* threshold of US$1,000.[53]

R17	Reliance on Third Parties

Section 6(6) of the Money Laundering and Financing of Terrorism (Prevention) Act, 2011 permits accountable institutions to rely on intermediaries or third parties to undertake their obligations under subsections 6(1) and 6(2), or to introduce business. The MLFTPA does not contain any provisions related to reliance by a financial institution on a third party that is part of the same financial group.

R18	Internal Controls

The new FATF Recommendation 18 introduces the requirement that financial groups should have group-wide AML/CFT programmes that include information sharing within the group. This is not sufficiently covered in the Money Laundering and Financing of Terrorism (Prevention) Act, 2011. Further, 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. This is also not covered in the Money Laundering and Financing of Terrorism (Prevention) Act 2011. In this regard, it is noted by ESAAMLG that, "this FATF Recommendation does not apply to the Kingdom of Swaziland since domestic financial institutions do not have foreign branches and subsidiaries operating in other jurisdiction(s)." It would however be wise to include such a provision in the MLFTPA in the event that one or more of Swaziland's accountable institutions, other than a bank, elect to expand their operations into other jurisdictions.

[52] Section 10(3).
[53] Interpretive Note to Recommendation 16, paragraph 5.