



Subject: Money Laundering and Financing of Terrorism

(Prevention) Guideline (AML/CFT) 2016

Number: 01

Circulated:

April 2016

Scope:

Insurers, Insurance Brokers, Insurance Agents, Retirement Funds, Investment Advisers, Manager of a Collective Investment Schemes, Dealers, Central Securities Depositories, Nominees, SACCOs, Money Lenders Lotteries, Pawn Brokers, Credit Provider, Credit Bureaus, Investment Adviser Representatives, Dealer Representatives, Securities Exchanges, Exempt Dealers, Hire-Purchase and any other Non-Bank Financial Services Provider as specified in the FSRA Act and non-bank financial services laws as amended from time to time.

Contents

Abbreviations	3
Definitions.....	4
1. Introduction	5
2. Background	6
2.1 FATF Recommendations and other International Financial Sector Standard Setting Bodies.	6
2.2 Fit and Proper Requirements.....	6
3. Key Concepts of the Guideline	7
3.1 Money Laundering	7
3.2 Financing of Terrorism.....	7
4. Underlying Principles.....	8
5. Assessment of Risks and Applying a Risk Based Approach	8
5.1 Risk Assessment.....	8
5.2 Risk Mitigation	9
5.3. New Products, Business Practices and Developing Technologies	10
6. Governance and Compliance.....	10
6.1 Role of the Board.....	10
6.2 Role of Senior Management	10
6.3 Responsibilities of the AMLO	11
7. Customer Due Diligence (CDD)	12
7.1 Anonymous or Fictitious persons	12
7.2 Reasonable suspicion prior to establishment of business relations	13
7.3 When CDD measures are to be performed.....	13
7.5 Identification of Customers.....	14
7.5.1 Natural Persons	14
7.5.2 Legal Persons	14
7.6 Verification of identity of natural persons appointed act on behalf of customer	16
7.7 Identification and Verification of Identity of Beneficial Owner	16
7.8 Ongoing Monitoring.....	16
7.9 Non-Face-to-Face Verification	17
7.10 Simplified Customer Due Diligence	18
7.11 Enhanced Customer Due Diligence	19
8. Politically Exposed Persons	20
9. Reliance On Third Parties	21
10. Record Keeping.....	22
10.1 Customer Due Diligence Records.....	22
10.2 Transaction records.....	22
10.3 Manner in Which Records May Be Kept.....	23
11. Suspicious Transaction Reporting.....	23
11.1 Tipping-off and confidentiality	24
12. Staff Training	25
13. Audit and Self-Assessment of Controls	26
14. Internal controls and foreign branches and subsidiaries.....	26
15. Sanctions for non-compliance with the Guideline.....	26
Appendix A - Examples of Suspicious Transactions	27
Non-Bank Financial Service Providers	27
Securities Dealers	28
Money Services Businesses	29
Appendix B STR Form.....	30

Abbreviations

AML	Anti-Money Laundering
AMLO	Anti-Money Laundering (reporting or compliance) Officer
AML/CFT	Anti Money Laundering and combating the financing of terrorism
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
FATF	Financial Action Task Force
FSRA	Financial Services Regulatory Authority
FSRA Act	Financial Services Regulatory Authority Act, 2010
FSP	Financial Services Provider
IAIS	International Association of Insurance Supervisors
IOPS	International Organization of Pension Supervisors
IOSCO	International Organization of Securities Commissions
ML	Money Laundering
MLFTP Act	Money Laundering and Financing of Terrorism (Prevention) Act, 2011
PEP	Politically Exposed Persons
SFIU	Swaziland Financial Intelligence Unit
STR	Suspicious Transaction Report

Definitions

For purposes of this Guideline:

Accountable Institution: - means an institution that carries on any business or activities as set out in section 2 of the Money Laundering and Financing of Terrorism (Prevention) Act, 6/2011 and includes all non-bank financial services providers as set out in the Second Schedule of the FSRA Act 2/2010.

AML/CFT Risk Management and Compliance Program – means the program referred to in paragraph 5.2.

Authority - means the Financial Services Regulatory Authority.

Beneficial owner– means the natural person(s) who independently or together with a connected person, directly or indirectly owns or controls a customer or the person on behalf of whom a transaction is being conducted.

Business relationship - means any business, professional or commercial arrangement or proposed arrangement where the purpose or effect of the arrangement is to facilitate a transaction on an occasional, frequent, habitual or regular basis between a customer and an accountable institution.

Customer–in relation to a transaction or an account includes;

- a) The person in whose name a transaction or account is arranged, opened or undertaken;
- b) A signatory to a transaction or account;
- c) Any person to whom a transaction has been assigned or transferred;
- d) Any person who is authorized to conduct a transaction; or
- e) Such other person as the Minister may by Notice published in the gazette prescribe.

Customer Due Diligence or CDD– means the measures taken to know and understand a customer and a beneficial owner of a customer which measures includes the process of collecting, analysing and verifying information in order to identify and verify identity of the customer or beneficial owner.

Financial Crime as defined by the FSRA Act, 2010 means –

- a) a crime that involves fraud or dishonesty relating to a financial services provider;
- b) financing or facilitating crime relating to a financial services provider;
- c) dealing with the proceeds of crime, whether or not related to a financial services provider;

- d) money laundering or
- e) financing terrorism;

Non-Bank Financial Services Provider – means any person mentioned in the second schedule of the FSRA Act, 2010 and/or prescribed in any non-bank financial services law in the first schedule of the FSRA Act, 2010;

Politically Exposed Person – means a person who holds, or has held, a prominent public position, whether in Swaziland or in a foreign country, including, but not limited to, a Head of State or Government; a politician at a national level; a senior Government official, judicial, military or party official at the national level; a senior executive of a state-owned enterprise, persons who are or have been entrusted with a prominent function by international organizations; or an individual or entity identified as having close family ties or personal or business connections to any of the aforementioned persons.

Authority – means the FSRA exercising its oversight mandate over accountable institutions for AML/CFT compliance in terms of section 35 of the MLTFP Act 6/2011.

Unlawful activity – means any act or omission which if committed in Swaziland or elsewhere would constitute a criminal offence.

1. Introduction

(a) The fight against financial crime is an ongoing priority for governments around the world. The financial services sector is potentially at risk of being misused for money laundering and the financing of terrorism. The financial services sector can be a target for money launderers and for those seeking resources for terrorism acts or for ways to process funds to accomplices. Financial services providers can be involved, knowingly or unknowingly, in money laundering and the financing of terrorism and this exposes them to legal, operational and reputational risk. It is therefore important for the non-bank financial services providers to take adequate measures to prevent being used by money launderers and terrorists and to address possible cases of money laundering and terrorist financing.

(b) This guideline is issued pursuant to:

- section 35 of the MLTFP Act which empowers the Authority to monitor and ensure that accountable institutions falling under its supervisory and regulatory purview comply with AML/CFT requirements;
- FATF Recommendation 34 which requires supervisors to establish guidelines which will assist accountable institutions in applying AML/CFT measures, in particular, in detecting and reporting suspicious and unusual transactions; and

- section 33 of the FSRA Act, 2010 which empowers the Authority to issue guidelines for providing guidance in furtherance of its regulatory objectives

(c) The MLFTP Act further provides for standards, processes, policies and procedures which should be adopted by accountable institutions to deter and detect money laundering and terrorist financing. Section 2 of the MLFTP Act defines accountable institutions and requires them to report suspicious transactions to the Swaziland Financial Intelligence Unit (SFIU). All entities providing financial services in terms of the FSRA Act are accountable institutions and are legally bound to comply with the provisions of MLFTP Act by putting in place effective and risk based AML/CFT frameworks to combat ML/TF risks in their businesses.

(d) The requirements of this guideline apply to accountable institutions falling under the supervisory and regulatory purview of the Authority.

2. Background

2.1 FATF Recommendations and other International Financial Sector Standard Setting Bodies.

(a) FATF is an inter-governmental body established with the mandate to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorism financing and the proliferation of weapons of mass destruction, and other threats to the integrity of the international financial system. FATF has developed recommendations on AML/CFT (collectively referred to here as “FATF Recommendations”). The Recommendations are the international standards which countries should implement taking into account their particular circumstances.¹

(b) The Authority is a member of other international standard setting bodies such as IAIS, IOPS and IOSCO and subscribes to international best practise by complying with principles set by these bodies. These standard setting bodies have given AML/CFT high priority and require supervisors and regulators to ensure that accountable institutions comply with FATF recommendations.

2.2 Fit and Proper Requirements

(a) FATF Recommendations include measures to mitigate the risk that criminals might take ownership of, or unduly influence the management of financial services providers. The screening of key functionaries is set out in the Authority’s “Fit and Proper and Rehabilitation Guideline and Rehabilitation Criteria 2015”.

¹FATF recommendations are available on the following website/link;
http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

(b) The Authority screens all persons who own or control, directly or indirectly, or have significant interests in the business of financial services providers. Screening is an ongoing process and it is done prior to the approval of a new license and when ownership interests change. However, the Authority also relies on the internal processes of financial services providers for assessing the ongoing suitability and integrity of key functionaries who are appointed after a license is issued.

3. Key Concepts of the Guideline

3.1 Money Laundering

(a) Money laundering is a process in which funds or property believed to be obtained directly or indirectly through illegal or criminal activities are converted into other assets so as to conceal their true origin or ownership. The main objective is to legitimize income originating from illegitimate sources so that it loses its criminal identity and appears to be legitimately derived.

(b) The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a financial services provider to the money laundering activity:

- Placement–Physical disposal of criminal proceeds or placing dirty money into the financial system via a cash deposit, such as purchasing a policy using cash as opposed to using banking channels or offering to top-up premiums, purchase of investments with cash, or repayment of an outstanding loan using dirty money.
- Layering–The separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the origin of funds and provide appearance of legitimacy, such as borrowing against an existing policy or an early surrender of an investment policy in circumstances where doing so defies economic logic.
- Integration–Placing the laundered proceeds back into the economy as apparently legitimate funds. For instance, with the proceeds from a surrendered insurance policy or redeemed shares or reimbursements, a launderer buys “clean” or legitimate fixed assets or registers a legitimate business in to which proceeds are deposited. The funds are then integrated back to criminal activities, such as drug trafficking.

3.2 Financing of Terrorism

(a) The financing of terrorism is an act of directly or indirectly providing, whether by giving, lending or otherwise making available or collecting, funds or property with the intention that they should be used, or having reasonable grounds to believe that they are to be used, in full or in part, in order to carry out an act of terrorism.

(b) Terrorism seeks to influence or compel governments or others into a particular course of action through the use of violence, damage to property, danger to life or serious risks to health. Terrorists require funds to carry out acts of terrorism, and terrorist financing provides the funds needed. The methods used by terrorists to move, collect, hide or make available funds for their activities are similar to those used by criminals to launder their funds.

4. Underlying Principles

This guideline is based on the principles that accountable institutions shall:

- Exercise due diligence when dealing with customers, persons appointed to act on a customer's behalf, beneficial owners and beneficiaries.
- Conduct business in conformity with high ethical standards and guard against undertaking any transaction that is or maybe connected with or may facilitate money laundering and terrorist financing.
- To the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Swaziland in preventing money laundering and terrorism financing.

5. Assessment of Risks and Applying a Risk Based Approach

5.1 Risk Assessment

(a) FATF Recommendation One requires accountable institutions to put in place appropriate processes to identify, assess, monitor, manage and mitigate money laundering and financing of terrorism risks affecting their businesses. These risks include, but are not limited to, risks that may arise in relation to the development of new products, business practices and delivery channels or risks that may arise through the use of new or developing technologies.

(b) The risk assessments should be documented as they serves as a basis for developing the accountable institution's AML/CFT Risk Management and Compliance Program. When identifying aspects of business that make an accountable institution susceptible to ML/TF risks the following factors should be considered:

- (a) the nature, size and complexity of the business;
- (b) type of customers and communities with whom they do business;
- (c) countries or jurisdictions from where customers come;
- (d) products and services offered;
- (e) delivery channels and business practices;
- (f) type of institutions the accountable institution has business dealings with; and
- (g) countries in which the accountable institution operates.

(c) The steps referred to in paragraph (a) should include:

- (a) having appropriate mechanisms in place for providing risk assessment information to the Authority, the SFIU and competent authorities;
- (b) reviewing the risk assessments annually to keep them up to date; and
- (c) auditing the risk assessment in terms of the MLTFP Act.

5.2 Risk Mitigation

(a) Accountable institutions are required to develop, document, maintain and implement an anti money laundering and countering the financing of terrorism risk management and compliance program (AML/CFT Risk Management and Compliance Program).

(b) An AML/CFT Risk Management and Compliance Program must:

(i) set out policies, procedures and controls that will enable the accountable institution to effectively manage and mitigate risks identified by the accountable institution or notified to it by the Authority or the SFIU;

(ii) be approved by senior management or other person or persons exercising the highest level of authority in the accountable institution;

(iii) provide for the manner in which and the processes by which –

- ❖ the identification and verification of customers is performed by the accountable institution;
- ❖ ongoing due diligence in respect of business relationships is conducted by the accountable institution;
- ❖ enhanced due diligence is performed by the accountable institution to address higher risks identified during the risk assessment;
- ❖ the accountable institution determines whether a prospective customer is a politically exposed person; and
- ❖ the AML/CFT Risk Management and Compliance Program is implemented in branches, subsidiaries and other operations of the accountable institution in foreign countries so as to enable the accountable institution to comply with its obligations under the MLTFP Act.

(iv) provide for the format in which records are kept by the accountable institution in terms of the MLTFP Act;

(v) enable the accountable institution to determine when a transaction is reportable to the SFIU in terms of paragraph 11.

(vi) be made available to relevant employees within the accountable institutions who have a responsibility to comply with the MLTFP Act; and

(vii) be submitted to the Authority or the SFIU, on request.

5.3. New Products, Business Practices and Developing Technologies

(a) Accountable institutions must identify and assess money laundering and terrorism financing risks that may arise in relation to the development of new products, business practices, new delivery channels and the use of new or developing technologies for both new and pre-existing products.

(b) Risk assessments should be undertaken prior to the launch or use of the products, business practices and technologies and accountable institutions should further take appropriate measures to manage and mitigate the risks.

(c) In complying with paragraphs (a) and (b), special attention should be given to any new products, business practices and delivery channels and new or developing technologies that favour anonymity.

6. Governance and Compliance

6.1 Role of the Board

(a) The Board of Directors of an accountable institution has oversight accountability for approving policies and procedures and monitoring the effectiveness of the AML/CFT Risk Management and Compliance Program on a regular basis. It is the responsibility of the Board to ensure compliance by an accountable institution and its employees with the provisions of the MLTFP Act and the accountable institution's AML/CFT Risk Management and Compliance Program.

(b) The Board should further align its governance and oversight practices with the FSRA Act, 2010 and sector specific legislation under the regulatory ambit of the Authority.

6.2 Role of Senior Management

(a) Senior Management is responsible and accountable for exercising oversight on the day-to-day implementation of the AML/CFT Risk Management and Compliance Program to ensure that it is adequate to mitigate ML/TF risks and that it is implemented effectively in all relevant business areas. Senior Management should ensure that:

- (i) an appropriately qualified person of sufficient competence and seniority is appointed as an AMLO;
- (ii) the Authority is notified in writing of the appointment of an AMLO and furnished with a detailed curriculum vita of the AMLO and a full description of the duties of the AMLO;

(iii) the AMLO is resident in Swaziland;

(iv) the Authority is informed in writing of the termination of services of an AMLO and provided with an explanation of the reasons for the termination, within 15 days of such termination;

(v) the AMLO is a member of Senior Management or reports directly to Senior Management or the Board of Directors and does not report to the internal auditor in order to avoid potential conflicts of responsibilities;

(vi) the AMLO has clear and documented responsibility and accountability for designing the AML/CFT Risk Management and Compliance Program ensuring that the accountable institution assesses the risk of ML/TF it may expect to face in the course of its business and uses the results of the risk assessment in designing the AML/CTF Risk Management and Compliance Program..

(vii) the AMLO and the internal auditor have adequate resources in terms of people, data management systems and budget to implement and administer the AML/CFT Risk Management and Compliance Program effectively and to offer objective advice to the Board and Senior Management; and

(viii) any recommendations made by the AMLO, the internal auditor and Senior Management in respect of the AML/CFT Risk Management and Compliance Program are acted upon in a timely manner.

(b) Senior Management should further ensure that they receive sufficient pertinent information from the AMLO, the internal auditor and other sources, as appropriate, to enable them to ensure the overall adequacy and effectiveness of the AML/CFT Risk Management and Compliance Program.

6.3 Responsibilities of the AMLO

(a) The responsibilities of the AMLO should, among others, include the following:

- ensuring that the AML/CFT risk assessment of the entity is developed, documented and approved by the Board;
- developing a risk based AML/CFT Risk Management and Compliance Program;
- keeping a register of all reports received from staff and a separate register of all reports made to the SFIU;
- ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorism financing is suspected;

- advising and training management, the Board (where relevant) and staff on the development and implementation of internal policies, procedures and controls on AML/CFT;
- carrying out, or overseeing the carrying out of, ongoing monitoring of the business relations and reviewing a sample of records and transactions for compliance with this Guideline and the MLFTP Act;
- promoting compliance with this Guideline, including observation of the underlying principles on AML/CFT and taking overall charge of all AML/CFT matters within the accountable institution;
- acting as a liaison officer between the accountable institution, the Authority and the SFIU; and
- developing and implementing a self-assessment of controls.

(b) The reports from the AMLO should include information on significant patterns or trends, self-assessment of controls and material changes thereto, as well as remedial action plans or recommendations, if any, with milestones and target dates for completion.

(c) Where appropriate, the AMLO should draw conclusions, offer advice and make recommendations about the overall structure and scope of the AML/CFT Risk Management and Compliance Program.

7. Customer Due Diligence (CDD)

An accountable institution shall before entering into a business relationship with any person, ascertain the identity of a customer or beneficial owner on the basis of any official 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 which is reasonably capable of verifying the identity of the customer or beneficial owner.

7.1 Anonymous or Fictitious persons

(a) An accountable institution should know its customers and shall not deal with any person on an anonymous basis or any person using a fictitious name and should give special attention to the risks arising from new or developing technologies that may favour anonymity of customers.

(b) Whenever an accountable institution engages with a prospective customer to enter into a transaction or to establish a business relationship, the accountable institution must, in the course of establishing that business relationship and in accordance with its AML/CFT Risk Management and Compliance Program –

- (a) establish and verify the identity of the customer; and

(b) if the customer is acting on behalf of another person, establish and verify the identity of that other person and the authority to establish the business relationship or to conclude the transaction on behalf of that other person; and

(c) if another person is acting on behalf of the customer, establish and verify the identity of that other person and that other person's authority to act on behalf of the customer.

7.2 Reasonable suspicion prior to establishment of business relations

If, prior to establishing business relations with a customer, an accountable institution has reasonable grounds to suspect that the assets or funds of a customer are proceeds related to the facilitation or carrying out the offence of terrorism as defined in the Suppression of Terrorism Act, 2008, the accountable institution shall -

(a) not establish business relations with, or undertake a transaction with the prospective customer; and

(b) file a suspicious transaction report to the SFIU.

7.3 When CDD measures are to be performed

(a) Accountable institutions shall perform CDD measures in accordance with this Guideline when:

- Establishing business relations with a customer;
- carrying out occasional transactions: above the applicable designated threshold E 10 000 (cash) and E20 000 (any other);
- carrying out transactions that are wire transfers;
- Dealing with a customer as part of an existing business relationship;
- There is a suspicion of money laundering or terrorist financing;
- the accountable institution has doubts about the veracity or adequacy of previously obtained customer identification data.

(b) Accountable institutions should carefully assess the specific background and other conditions and needs of the customer. To achieve this, an accountable institution should collect relevant information, for example, type and background of the customer or beneficial owner, income and details of sources of funds. This will lead to a customer risk profile, which could serve as a reference to establish the purpose of the transaction and to monitor subsequent transactions and events.

(c) Where an accountable institution suspects that two or more transactions are or may be related, linked or the result of the deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the threshold measures set out in paragraph 7.3 (a) above, the

accountable institution shall treat the transactions as a single transaction and aggregate the values of the transactions in order to comply with this Guideline.

7.4 CDD measures when business relations are being established

Factors to be considered when creating a customer risk profile include but are not limited to:

- type and background of the customer or beneficial owner;
- geographic sphere of the activities of the customer and/or beneficial owner;
- nature of the business activities;
- sources of funds;
- sources of wealth;
- customer's and/or beneficial owner's geographical base;
- frequency and scale of activity;
- whether or not payments will be made to third parties;
- type and complexity of the business relationship; and
- size and pattern of transactions.

7.5 Identification of Customers

Accountable institutions are required to identify and verify the identity of each customer who applies to them to establish business relations using reliable and independent source documents data and information.

7.5.1 Natural Persons

Where a customer is a natural person, the accountable institution should obtain and record information regarding the customer, including but not limited to the following:

- full legal name(s) used, including any aliases;
- occupation, public position held and name of employer (if self-employed, the nature of self-employment);
- specimen signature;
- residential address and contact telephone number;
- nationality;
- date and place of birth;
- national identity card; and
- tax identification number;

7.5.2 Legal Persons

(a) For customers who are legal persons such as companies, partnerships, trusts, associations or other legal arrangements, CDD will require identification of the natural persons who comprise the mind and management of the legal person. This means that the accountable institution should understand the ownership and control structure of the customer.

(b) Apart from identifying the customer, the following should also be identified:

- each natural person who independently or together with a connected person has a controlling ownership interest in the legal person or who otherwise exercises control over the management of the legal person including the capacity in which the natural person is representing the legal person;
- the beneficial owner of the customer;
- tax identification number of the customer;
- founding instruments in terms of which the legal person is created;
- place of incorporation or registration;
- date of incorporation or registration;
- registered address of the legal person or address from which the entity operates; and
- shareholders or persons having executive authority in the legal person; and
- residential address and contact particulars of each shareholder, partner, trustee, beneficiary or person having executive authority in the legal person.

(c) In the case of a partnership or similar arrangement, the accountable institution should further identify and establish the natural person purporting to enter into a transaction or to establish a business relationship on behalf of the partnership. Furthermore, the name of the partnership, the identity of every partner and the person who exercises executive control over the partnership should also be established.

(d) In the case of a trust or similar arrangement, the accountable institution should further identify and establish the name of the trust, and the identity of the founder and each trustee and natural person who purports to be authorised to enter into a transaction or to establish a business relationship on behalf of the trust. Each beneficiary referred to in the trust deed or other founding instrument and the particulars of how the beneficiaries are determined should also be established by the accountable institution.

7.6 Verification of identity of natural persons appointed act on behalf of customer

(a) Where the customer appoints one or more natural persons to act on its behalf in establishing business relations with the accountable institution, or the customer is not a natural person, the accountable institution should:

- Identify the natural person(s) that act or are appointed to act on behalf of the customer, as if such persons were themselves customers;
- verify the identity of these persons using reliable, independent source documents;
- retain copies of all reference documents used to verify the identity of these persons; and
- verify the authority of such persons to act on behalf of the customer by obtaining appropriate documentary evidence of their appointment, for example. e.g. power of Attorney, letters of administration for appointment as executor and court orders for appointment as curators;

(b) Where the customer is a Swaziland Government entity, the accountable institution is required to obtain such information as may be required to confirm that the customer is a Swaziland Government entity as asserted for example, a confirmation letter from the responsible ministry with an official seal/stamp.

7.7 Identification and Verification of Identity of Beneficial Owner

Accountable institutions are required to inquire if any beneficial owner exists in relation to a customer. Where there is one or more beneficial owner in relation to a customer, the accountable institution should take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner.

When an accountable institution establishes and verifies the identity of the beneficial owner of a legal person the institution must –

(a) identify and verify each natural persons who, independently or together with a connected person, has a controlling ownership interest or ultimately owns the legal person; and

(b) if there is doubt as to whether a natural person contemplated in paragraph (a) is a beneficial owner of the legal person in question or where no natural persons ultimately own the legal person, identify each natural person who ultimately control the legal person or who otherwise exercises executive control or management or similar position in the legal person.

7.8 Ongoing Monitoring

(a) Accountable institutions should pay attention to all requested changes that occur after the business relationship has been established. They should monitor on an ongoing basis their business relations

with customers and should observe and assess the activity in respect of the customer and scrutinize transactions undertaken to ensure that they are consistent with the accountable institution's knowledge of the consumer, its business and risk profile and where appropriate, the sources of funds.

(b) Accountable institutions should pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent economic or lawful purpose. To the extent possible, accountable institutions should inquire into the background and purpose of all such transactions and document their findings with a view to making this information available to the SFIU should the need arise.

(c) Periodic reviews of customer identification information obtained should be done to ensure that the information is kept up to date, particularly for higher-risk categories of customers.

(d) For the purpose of ongoing monitoring, an accountable institution should put in place and implement adequate systems and processes, commensurate with the size and complexity of the accountable institution, to –

(i) monitor its business relations with customers; and

(ii) detect and report suspicious, complex, unusually large or unusual patterns of transactions.

(e) Where there are any reasonable grounds for suspecting that existing business relations with a customer are connected to money laundering or the financing of terrorism, and where the accountable institution considers it appropriate to retain the customer it should –

(i) substantiate and document the reasons for retaining the customer; and

(ii) subject the accountable institution's business relations with the customer to enhanced risk mitigation measures, including enhanced on-going monitoring.

7.9 Non-Face-to-Face Verification

(a) Accountable institutions should put in place policies and procedures to address specific risks associated with non-face-to-face business relationships or transactions, which should be implemented when establishing business relations and transacting through instructions conveyed by customers over the post, telephone or internet.

(b) Where there is no face-to-face contact, the accountable institution should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.

(c) As a guide, the following measures should be considered to mitigate the heightened risk associated with not being able to have face-to-face contact when establishing business relations:

- telephone contact with the customer at a residential or business number that can be verified independently;
- confirmation of the customer's address through an exchange of correspondence or another appropriate method;
- subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer at a listed business number of the employer;
- confirmation of the customer's salary details by requiring the presentation of recent bank statements;
- requiring the customer to make an initial payment using a cheque drawn from the customer's personal account; and
- other reliable verification checks adopted by the accountable institution for non-face-to-face business.

7.10 Simplified Customer Due Diligence

(a) Where the risks of money laundering and terrorism financing are lower, accountable institutions may apply simplified CDD measures. The simplified measures must have been identified through a risk assessment and should be commensurate with the lower risk factors having regard to the circumstances of each case. This means that the accountable institution must have a basis for applying simplified CDD measures.

(b) Some examples of possible simplified measures are:

- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable money threshold; and
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

(c) Some examples of when an accountable institution might apply reduced CDD measures are where:

- reliable information on the customer and beneficial owner is publicly available or where adequate checks and controls exist elsewhere in the national system;
- the accountable institution is dealing with another accountable institution whose AML/CFT controls it is familiar with by virtue of previous dealings; or

- the customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;
- the customer poses a lower risk of ML/TF because of the nature of the product that the customer has bought or intends to buy such as a micro insurance product or a micro credit loan.

(d) Where simplified CDD measures have been performed in relation to a customer, the accountable institution should document:

- (i) the details of its risk assessment; and
- (ii) the nature of the simplified CDD measures.

(e) Simplified CDD measures are not allowed where there is a suspicion of money laundering and terrorist financing or where specific higher risk scenarios apply.

7.11 Enhanced Customer Due Diligence

(a) Accountable institutions shall implement appropriate internal risk management systems, policies procedures and controls to determine if business relations with or transactions for any customer present a higher risk for money laundering or terrorism financing.

(b) Enhanced CDD measures refers to additional due diligence measures that must be applied where the customer has not been physically present for identification or where the customer is politically exposed or in any situation which by its nature can present a higher risk of money laundering or terrorism financing. These measures should apply to all higher-risk business relationships, customers and transactions.

(c) Entities should examine the background and purpose of all complex or unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, they should increase the nature and intensity of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

(d) Circumstances where a customer presents or may present a higher risk for money laundering or terrorism financing may include the following:

- (i) where a customer or beneficial owner of a customer is from or in a country in relation to which FATF has called for countermeasures, the accountable institution shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering and terrorism financing; and

- (ii) where a customer or beneficial owner of the customer is from or in a country known to have inadequate AML/CFT measures, as determined by the accountable institution or notified to the

accountable institution by the Authority or other foreign or local regulatory bodies, the accountable institution shall assess whether such customer presents a higher risk for money laundering and terrorism financing.

8. Politically Exposed Persons

(a) The FATF Recommendations require additional due diligence measures in relation to Politically Exposed Persons (PEPs).

(b) Accountable institutions should take note that PEPs can be foreign, domestic or may be persons who are or have been entrusted with a prominent function by international organizations. Therefore in addition to performing CDD measures specified in paragraph 7, accountable institutions should perform enhanced CDD measures in relation to such customers. For this purpose accountable institutions should:

- put in place appropriate risk management systems, internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;
- establish a board-approved customer acceptance policy with regard to PEPs, taking account of the reputational and other risks involved;
- obtain approval from senior management to establish or continue business relations with such customers;
- establish, by appropriate and reasonable means, the source of wealth and source of funds of such customers; and
- conduct enhanced ongoing monitoring of the business relations with the customer.

(c) Accountable institutions are also required to give particular attention to business relations and transactions with persons from countries that have inadequate AML/CFT measures. For this purpose they may take a range of steps, including the adoption of measures similar to those applied to PEPs and other high-risk categories.

(d) Determining whether an individual is a PEP may not always be straightforward. In the circumstances, the Authority considers it acceptable for accountable institutions to refer to databases of PEPs (available on the internet). However, the Authority also expects accountable institutions to exercise a measure of discretion and sound judgment in deciding whether an individual who is not on such a database should nevertheless be treated as a PEP, having regard to the risks and the circumstances of each case.

(e) Enhanced CDD measures must also be applied to immediate family members and known close associates of PEPs. An immediate family member include spouse, previous spouse, life partner, children and step children and their spouses or life partners, parents, siblings and step siblings and their spouses or life partners.

(f) In relation to life insurance policies, accountable institutions should take reasonable measures to determine whether the beneficiaries and the beneficial owners of the beneficiaries if any, are PEPs. This determination should be made at claims stage. Where higher risks are identified accountable institutions should:

- (i) require that senior management be informed before the payment of the policy proceeds is made;
- (ii) conduct enhanced scrutiny of the whole business relationship with the policyholder; and
- (iii) consider making a suspicious transaction report.

9. Reliance On Third Parties

(a) Accountable institutions are allowed to rely on intermediaries or other third parties to perform some elements of the CDD process, provided that the following requirements are met:

- (i) the accountable institution must be satisfied that the third party it intends to rely upon is subject to and is supervised for compliance with AML/CFT requirements consistent with the standards set by the FATF, and has adequate AML/CFT systems in place to comply with those requirements;
- (ii) the third party is able and willing to provide to the accountable institution without delay, any identification data, documents or information obtained by the third party relating to CDD measures applied on customers and beneficial owners;
- (iii) the third party commits in writing that it shall perform CDD measures, grant the accountable institution access to CDD documentation in its custody and report to the SFIU and the accountable institution in the case of a suspicious or unusual transaction; and
- (iv) the accountable institution undertakes and completes its own verification of the customer and beneficial owner if it has doubts that appropriate due diligence was performed by the third party.

(b) For the avoidance of doubt, notwithstanding the reliance on a third party, the ultimate responsibility for the customer and beneficial owner identification and verification remains with the accountable institution relying on a third party. However, third parties are responsible for the validity of all information obtained.

10. Record Keeping

10.1 Customer Due Diligence Records

(a) Accountable institutions must keep all records obtained or generated by CDD measures, including account files, business correspondence and results of any analysis undertaken. Other records are the risk profile of each customer and beneficial owner and copies of identification documents.

(b) In the case of a business relationship, the records must reflect the information obtained by the accountable institution describing the nature of the business relationship concerned, the intended purpose of the business relationship and the source of the funds which the prospective customer is expected to use in concluding transactions in the course of the business relationship. Records must be kept for a period of five years from the date on which the business relationship is terminated.

10.2 Transaction records

(a) Accountable institutions must keep a record of every domestic or international transaction, whether the transaction is a single transaction or concluded in the course of an ongoing business relationship with the customer. The transaction records must be sufficient to enable the transaction to be readily reconstructed at any time, to provide evidence for prosecution of any offence and to assess the level of compliance with this Guideline. The records must include at least the following information:

(i) the amount involved and the currency in which it was denominated;

(ii) the date on which the transaction was concluded;

(iii) the parties to the transaction;

(iv) the nature of the transaction; and

(v) if the accountable institution provides account facilities to its customers, the identifying particulars of all accounts that are involved in the transaction.

(b) Records that relate to a transaction which is concluded must be kept for at least five years from the date on which the transaction was concluded. On the other hand, records that relate to a

transaction which gave rise to a suspicious or unusual transaction report must be kept for at least five years from the date on which the report was submitted to the SFIU.

(c) Accountable institutions shall further maintain specific records beyond the minimum period of five years when requested to do so by the SFIU, a law enforcement agency or the Authority.

10.3 Manner in Which Records May Be Kept

(a) Accountable institutions may use the services of a third party for keeping and maintaining of records as long as the accountable institution has free and easy access to the records and the records are readily available to the internal and external auditors, the SFIU and the Authority.

(b) Where an accountable institution relies on a third party to keep and maintain records on its behalf, the accountable institution must provide the SFIU and the Authority with the following particulars of the third party:

(i) registered name;

(ii) name under which the third party conducts business;

(iii) name and contact particulars of individual who exercises control over access to the records;

(iv) address where records are kept;

(v) address from where the third party exercises control over the records; and

(vi) name and particulars of the individual(s) or the third party who liaise with the accountable institution concerning the records and their retention..

(c) For the avoidance of doubt, the ultimate responsibility for ensuring that records are kept and maintained in the manner set out in this paragraph, lies with the accountable institution which shall also be liable for failure to meet the requirements.

(d) Records may be kept in electronic form, provided that they are capable of being reproduced in a legible format which will be admissible in a court of law in Swaziland.

11. Suspicious Transaction Reporting

(a) If an accountable institution suspects or has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of a criminal activity, money

laundering or terrorism financing or that funds are proceeds of a criminal activity or are related to terrorist financing, it is required to report its suspicion promptly to the SFIU.

(b) All suspicious or unusual transactions must be reported to the SFIU within two days of forming the suspicion regardless of the amount of the transaction or funds involved.

(c) The Authority requires institutions to have adequate processes and systems for detecting and identifying suspicious transactions and internal processes for evaluating whether a matter should be referred to the SFIU.

(d) An important pre-condition for the recognition of a suspicious transaction is for the accountable institution to know enough about the customer and business relationship to recognize that a transaction is, or a series of transactions are, unusual or suspicious.

(e) In order to meet its obligations, an accountable institution is required to:

- establish a single reference point within the organization to whom all staff and representatives are instructed to promptly refer all transactions suspected of being connected with money laundering or terrorist financing. This involves putting in place a clear process and procedure for ensuring that all suspicious and unusual transaction are reported through the AMLO to the SFIU.
- document the policy and procedures for reporting to the AMLO so that employees know what should be reported and the process to follow when reporting; and
- keep records of all transactions referred to the SFIU together with all internal findings and analysis done in relation to any suspicious transactions, including transactions that are not reported to the SFIU.

(f) Examples of suspicious transactions are set out in Appendix A to this Guideline. These examples are not exhaustive and are only examples of the most basic ways money may be laundered. If any transactions similar to those in Appendix A, or any other suspicious transactions, are identified, this should prompt further enquiries and, where necessary, investigations into the source of funds.

11.1 Tipping-off and confidentiality

(a) Accountable institutions and directors, officers, employees and auditors of accountable institutions are:

- (i) prohibited from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the SFIU; and

(ii) protected from civil, criminal or disciplinary proceedings if they report their suspicions in good faith to the SFIU, even if they did not know precisely what the suspected criminal activity was, and regardless of whether illegal activity actually occurred.

(b) A risk exists that customers could be unintentionally tipped-off when accountable institutions perform their CDD obligations. A customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing activity. Therefore, if the accountable institution forms a suspicion that a transaction or transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process.

12. Staff Training

(a) Accountable institutions should ensure that officers, employees and representatives have the necessary level of ability and integrity for performing their duties taking into account potential conflicts of interests and other relevant factors, such as the financial background of the employee. Entities should note that the responsibility for initial and on-going assessment of the fitness and propriety of staff lies with the entity.

(b) Accountable institutions are further required to keep records on the identification data obtained about key staff. It is therefore important that adequate screening procedures are put in place to ensure high standards when hiring employees.

(c) Officers, employees and representatives of accountable institutions should receive initial and ongoing training on;

(i) AML/CFT legislation, regulations, and in particular, CDD measures and detecting and reporting suspicious and unusual transactions;

(ii),the entity's policies, procedures and controls on AML/CFT;

(iii) the roles and responsibilities of officers, employees and representatives in combating money laundering and terrorism financing in terms of the AML/CFT legislation; and

(iv) prevailing trends, developments and techniques and trends on money laundering and terrorism financing.

(d) To ensure the effectiveness of training, entities should train relevant staff ensuring that training is tailor-made for the AML/CFT responsibilities of those particular staff members, monitor attendance at such training and take appropriate follow-up action in relation to staff.

(e) Records of all training undertaken, the content of the training program, names and qualifications of the facilitators and the lists of attendees should be kept for a minimum period of five years from the date of the training.

13. Audit and Self-Assessment of Controls

(a) Accountable institutions should maintain an adequately-resourced and independent audit function to test compliance with policies, procedures and controls. The assessment of AML/CFT controls is an important component of the AML/CFT Risk Management Program because of its quality assurance outcome. Entities should perform a self-assessment of control measures annually, which at a minimum covers the adequacy of risk assessment, AML/CFT policies and procedures, training and other controls implemented to mitigate money laundering and terrorism financing risks.

(b) Like the assessment of other risk management controls, effectiveness testing of the AML/CFT Risk Management Program is important and it should be planned and performed by an auditor(s) who has appropriate training and experience in respect of money laundering and terrorism financing risk and an appropriate level of knowledge of the regulatory requirements and guidelines.

14. Internal controls and foreign branches and subsidiaries

Accountable institutions that are part of a group implement group wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes. Entities should ensure that their foreign branches and subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against ML/TF.

15. Sanctions for non-compliance with the Guideline

Non-compliance with the Guideline will expose accountable institutions to disciplinary action in terms of section 35 of the Money Laundering and Terrorism Financing (Prevention) Act 6/2011 read *in tandem* with sections 67 and 68 of the FSRA Act. Accountable institutions should further note that compliance with the Guideline does not constitute a defence for prosecution for an offence under the MLTFP Act and/or under the FSRA Act. Therefore, entities are encouraged to take steps to ensure that they comply with the Guideline, the MLTFP Act and the FSRA Act.

Appendix A - Examples of Suspicious Transactions

Non-Bank Financial Service Providers

Accountable institutions that provide life insurance or annuities should consider the following indicators of potentially suspicious transactions:

- Customer wants to use cash for a large transaction;
- Customer proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account;
- Customer requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;
- Customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
- Customer conducts a transaction that results in a conspicuous increase in investment contributions;
- Scale of investment in insurance products is inconsistent with the client's economic profile;
- Unanticipated and inconsistent modification of customer's contractual conditions, including significant or regular premium top-ups;
- Unforeseen deposit of funds or abrupt withdrawal of funds;
- Involvement of one or more third parties in paying the premiums or in any other matters involving the policy;
- Overpayment of a policy premium with a subsequent request to refund the surplus to a third party;
- Funds used to pay policy premiums or deposits originate from different sources;
- Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions.
- Customer cancels investment or insurance soon after purchase;
- Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner;
- Customer shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract;

- Customer makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment;
- The first (or single) premium is paid from a bank account outside the country;
- Repeated and unexplained changes in beneficiary;
- Relationship between the policy holder and the beneficiary is not clearly established.

Securities Dealers

Accountable institutions that are involved in the business of dealing in securities, segregated fund products or any other financial instruments, including portfolio managers and investment counsellors, should consider the following indicators of potentially suspicious transactions;

- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or the customer's financial ability;
- Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed;
- Customer attempts to purchase investments with cash;
- Customer uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the customer or the customer's financial ability;
- Customer wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the customer;
- Customer frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the customer;
- Customer makes large or unusual settlements of securities in cash;
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading;
- Transfers of funds or securities between accounts not known to be related to the customer;
- Several customers open accounts within a short period of time to trade the same stock;
- Customer is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party;
- Unrelated customers redirect funds toward the same account;
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;
- Transaction of very large monetary size;
- Customer is willing to deposit or invest at rates that are not advantageous or competitive.

Money Services Businesses

Accountable institutions that are involved in the money services business, including foreign exchange dealers, money remitters, and issuers of traveller's cheques consider the following indicators of potentially suspicious transactions.

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate;
- Customer wants to pay transaction fees that exceed the posted fees;
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency;
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument;
- Customer wants a cheque issued in the same currency to replace the one being cashed.

Credit Providers and SACCOs

- In terms of a pawn broking transaction; the title of property pledged by the customer appears not to be authentic.
- The value of the property pledged by the customer appears to be significantly less than what it appears to be.
- Customer pledges property with no intention to settle and buy back.
- Customer borrows funds on behalf of a third party.
- Customer suddenly settles a loan in full.
- Repayment by a guarantor or third party under abnormal circumstances.
- Third parties settling higher purchase contracts on behalf of account holders.
- Frequent multiple deposits to member savings accounts.
- Borrowing large amounts of funds against member non-withdrawable savings and pledging to repay using unexplained funds (outside normal salary sources).
- Lump sum deposits to member savings accounts.

Appendix B STR Form

TO: The Financial Intelligence Unit
Development House
Swazi Plaza

REPORTING OF SUSPICIOUS MONEY LAUNDERING TRANSACTIONS AND TERRORISM
FINANCING ACTIVITIES PURSUANT TO THE MONEY LAUNDERING AND FINANCING OF
TERRORISM (PREVENTION) ACT, 6/
2011

FIU	REPORTING FORM			
TYPE OF REPORT:	✓ STR ☐	☐	☐	☐

Details of Disclosing Organisation:		
Name of Organisation*:		
Branch or Outlet:		If bank code :
Business area of Branch Outlet:		
Your Disclosure Ref:		
Date disclosure sent to Central Bank:		
<i>*If this is the first report your institution has made you MUST complete a separate form registering you as the compliance/money laundering officer.</i>		

Person subject of disclosure:		
Has a previous disclosed been made on this subject:		If Yes STR Ref:

Family name:		Title:	
Given Names(s):		Gender:	
Date of Birth:			
ID Document details:			
Address No. & Street:			
City or Town:			
Region:			
Post No :			
Country:			
Employer:			
Occupation:			

OR Company subject of disclosure:		
Company Name:		
Company No:		
Tax Number:		
Type of Business:		
Country of Reg:		
1. Registered Office Address No. & Street:		
City or Town:		
Region:		
Post No :		
Country:		
2. Trading Address No. & Street:		Is this address the same as 1.above?
City or Town:		
Region:		
Post No:		
Country:		

Other Information not contained in above felds:	
---	--

Financial Summary Overview:

Institution Name:			
Outlet / Branch:			
Date Opened:		Date if Closed :	
Customers Turnover:		Turnover time period:	
Customer A/C or Ref No:			
Balance held:		Date of Balance:	

Financial Summary Details:

Date:		Credit or Debit:	
Value:		Currency:	
Cash: Yes or No:		If No: type of financial instrument:	
Counterparty Name:			
Counterparty Institution:			
If bank, bank code:			

Date:		Credit or Debit:	
Value:		Currency:	
Cash: Yes or No:		If No: type of financial instrument:	
Counterparty Name:			
Counterparty Institution:			
If bank, bank code:			

Date:		Credit or Debit:	
Value:		Currency:	
Cash: Yes or No:		If No: type of financial instrument:	
Counterparty Name:			
Counterparty Institution:			
If bank, bank code:			

Date:		Credit or Debit:	
Value:		Currency:	
Cash: Yes or No:		If No: type of financial instrument:	
Counterparty Name:			
Counterparty Institution:			
If bank, bank code:			

Date:		Credit or Debit:	
Value:		Currency:	
Cash: Yes or No:		If No: type of financial instrument:	
Counterparty Name:			
Counterparty Institution:			
If bank, bank code:			

USE ADDITIONAL SHEETS IF THERE FURTHER DETAILS TO BE SHOWN.
And complete the following: Financial Summary SHEET No: of .

(Example: Sheet 2 of 2. This would include the first sheet plus one extra)

ASSOCIATED Person (with subject of disclosure):

Associated Person:			
Has a previous disclosed been made on this subject:			If Yes FIU Ref:
Family name:		Title:	
Given Names(s):		Gender:	
Date of Birth:			
ID Document details:			
Address No. & Street:			
City or Town:			
Region:			
Post No:			
Country:			
Employer:			
Occupation:			

<u>OR</u>	
<u>Associated Company:</u>	
Company Name:	
Company No:	
Tax Number:	
Type of Business:	
Country of Reg:	
1. Registered Office	
Address No. & Street:	
City or Town:	
Region:	
Post No:	
Country:	
2. Trading Address	
No. & Street:	
City or Town:	
Region:	
Post No:	
Country:	

Other Information not contained in above fields:	
--	--

USE ADDITIONAL COPIES OF THIS SHEETS IF THERE OTHER ASSOCIATED PEOPLE OR COMPANIES

Complete the following if addition associated person or company sheets are used:

ASSOCIATE SHEET No: of .

(Example: Sheet 2 of 2. This would include this sheet plus one extra)

Reason for Suspicion:

