Bank Use Promotion and Suppression of Money Laundering Unit

GUIDELINES ON ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM FOR SECURITIES MARKET PLAYERS, 2012

[Issued in terms of the Bank Use Promotion & Suppression of Money Laundering Act [Chapter 24:24]

These guidelines amplify and explain obligations that Securities Market Players are required to comply with under the Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24.24] (hereinafter referred to as "the Act").

The guidelines are issued in terms of the Act and are legally binding. They lay down the minimum standards on Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for Securities Market Players.

TABLE OF CONTENTS

Terms and Acronyms Used

Terms	Definition
AML / CFT	Anti Money Laundering and Combating Financing of Terrorism
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
BUP & FI Unit	Bank Use Promotion and Financial Intelligence Unit, also known as the Financial Intelligence Unit (FIU)
BUPSML Act	Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24]
Business Relationship	'Business relationship' is any arrangement between the designated institution and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
Designated Institution	Means any institution designated in terms of the Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24] for purposes of implementing statutory AML / CFT obligations prescribed therein, and includes an individual or entity carrying on the business of a Securities Market Player.
Money Laundering	is defined as an activity, which has or likely has the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.
Securities Market Players	Means any person (individual or corporate) who engages in the business of buying and selling of securities.
Shell Banks	means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.
STR	Suspicious Transaction Report
Suspicious Transaction	is a transaction which is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale. It is a transaction which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods or terrorism.
Terrorist financing	Terrorist financing (FT) includes the financing of terrorist acts, of terrorists and terrorist organisations.

1 INTRODUCTION

1.1 General Overview

1.1.1 Zimbabwe is a member of the Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG). ESAAMLG, along with other similar regional groups, is an associate member of the Financial Action Task Force (FATF). The FATF is an intergovernmental body tasked with setting standards and measures relating to Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) and overseeing their implementation by countries.

1.1.2 ESAAMLG and FATF members have undertaken to implement AML/CFT measures in their jurisdictions, guided by the FATF Recommendations, as amended from time to time.

1.1.3 In line with Zimbabwe's international obligations and the country's commitment to play its part in the national, regional and global fight against money laundering and terrorist financing, the country has put in place a legal and institutional framework designed to make it more difficult for criminals to use the country's financial system to launder proceeds of their criminal activities or to channel funds for the financing of terrorist activities.

1.1.4 The government has enacted various pieces of legislation, among which is the Bank Use Promotion & Suppression of Money Laundering Act [Chapter 24:24] (hereinafter the "BUPSML Act" or simply "the Act"); The Serious Offences Act [Chapter 9:07]; and the Suppression of Foreign and International Terrorism Act [Chapter 11:17].

1.1.5 The BUPSML Act imposes certain obligations on designated institutions and establishes a financial intelligence unit named the Bank Use Promotion and Suppression of Money Laundering Unit (hereinafter referred to as the "BUPSML Unit" or simply "the Unit"), or the FIU, whose main responsibility is to oversee compliance with the Act.

1.1.6 The BUPSML Unit is empowered to issue guidelines to amplify and give effect to the provisions of the BUPSML Act.

1.1.7 It is against this background that the Unit has issued these Guidelines, known as the Anti Money Laundering and Combating the Financing of Terrorism

Guidelines for Securities Market Players, 2012 (hereinafter simply referred to as “the Guidelines”).

1.2 What is Money Laundering & Terrorist Financing?

1.2.1 Money Laundering is any act or transaction that is designed to disguise the illegal source of proceeds of crime so that it looks like the funds came from a legitimate source.

1.2.2 There are various methods of laundering proceeds of crime; including the purchase of securities at a higher price and then selling them at a considerable loss to another party, and purchasing high value assets such as real estate.

1.2.3 For money laundering to take place, an offence or offences would have been committed from which the criminals derived a financial benefit. The offence from which the funds have been derived is called the “predicate offence”. Predicate offences to money laundering include all offences defined as “serious offence” in terms of the Serious Offences (Confiscation of Profits) Act. They include theft, fraud, drug trafficking, human trafficking, corruption, among many others.

1.2.4 The objective behind money laundering is that the criminals or their accomplices want to “clean up” proceeds of crime so that the funds don’t appear to be connected with the predicate offence.

1.2.5 The person laundering funds may or may not have been directly involved in the predicate offence.

1.2.6 The offence of financing of terrorism is, however, different from the offence of money laundering in that, with financing of terrorism, the funds are not necessarily linked to a predicate offence. Funds used to finance terrorism may come either from a legitimate or illegitimate source.

1.2.7 The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organizations.

1.2.8 Criminals favour using financial systems of countries to clean up and disguise the illicit origins of proceeds of crime. Similarly individuals and entities who

finance terrorism around the world also find it convenient to use the financial systems of countries to move funds that are used to finance terrorism.

1.2.9 Zimbabwe, like the majority of countries the world over, has put in place a framework designed to make it more difficult for criminals to use the country's financial system to either launder proceeds of crime or to finance terrorism.

1.2.10 It is in this context, that the law requires financial and other institutions favoured by money-launderers and financers of terrorism to implement AML/CFT measures, including submitting Suspicious Transaction Reports (STRs) to the FIU.

1.2.11 The offence of money laundering is criminalized in terms of the Serious Offences (Confiscation of Profits) Act while the offence of financing of terrorism is criminalised in terms of the Suppression of Foreign and International Terrorism Act.

1.2.12 The Bank Use Promotion and Suppression of Money Laundering Act sets out the measures that designated institutions are required to implement to combat money laundering and financing of terrorism.

1.3 The Role of the Financial Intelligence Unit (FIU)

1.3.1 The main statutory function of the FIU is to enforce compliance with Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT) legislation by designated institutions.

1.3.2 More particularly**,** the Unit is responsible for –

a) Receiving STRs from designated institutions;
b) Analyzing the received STRs;
c) Disseminating STRs of interest to law enforcement agencies;
d) Supervising and monitoring designated institutions to enforce compliance with the Act and the Guidelines.

1.4 What are Designated Institutions?

1.4.1 Designated institutions are those institutions specified in the BUPSML Act that are required to submit STRs and to put in place other specified AML/CFT measures.

1.4.2 Designated institutions include, but not limited to; –

Banks; insurance companies; legal practitioners; public accountants; estate agents, moneylenders, pension funds; asset managers; bureau de change, money transfer agencies and securities market players.

1.4.3 For the purposes of this Guideline, designated institutions refer to Securities Market Players (SMP).

1.5 Definition of Customer

1.5.1 In relation to SMPs, a 'Customer' is defined as:

"An individual or legal person who participates in the trading of securities."

1.6 Securities Market Players (SMPs)

1.6.1 The securities industry, along with banking and insurance, is one of the core industries through which persons and entities can access the financial system. This access provides opportunities for criminals to misuse the financial system to engage in money laundering (ML) and terrorist financing (TF).

1.6.2 Major Securities Market Players, as per this Guideline, are:

a) Stockbrokers
b) Investment banks – Merchant Banks, Discount Houses, Commercial Banks
c) Registered stock exchange
d) Transfer secretaries
e) Securities investment advisors
f) Securities custodians
g) Securities dealers

h) Any other institutions registered by the Securities and Exchange Commission to perform specific functions in the Securities Market.

1.6.3 Products traded on the Securities Market are, but not limited to the following:

a) Stocks/shares
b) Derivatives
c) Government securities
d) Unit trusts
e) Mutual funds
f) Bonds
g) Debentures
h) Depository receipts
i) Warrants
j) Any other products as defined in the Securities Act (Chapter 24:25).

1.6.4 These products are susceptible to money laundering or terrorist financing.

1.6.5 Therefore, the objective of prescribing this AML/CFT guideline is to prevent SMPs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

2 CUSTOMER DUE DILIGENCE (CDD) & KNOW YOUR CUSTOMER (KYC) PRINCIPLE

2.1 General

2.1.1 Customer Due Diligence (CDD) and Know Your Customer (KYC) are key elements in the fight against money laundering and terrorist financing. These elements enable SMPs to know/understand their customers and their financial dealings better, which in turn helps them identify suspicious transactions and manage risks prudently.

2.1.2 Securities Market Players are required to exercise Customer Due Diligence. Customer due diligence includes identifying, verifying and monitoring all

aspects of the applicant's identity, residential address, any temporary address, and includes information on the source of funds and source of wealth.

It also includes information relating to any beneficial owner who has an interest in the securities, or controller who exercises influence over the investment.

2.1.3 SMPs shall undertake CDD measures when:

a) business relationship is established;

i) carrying out occasional transactions above the threshold that will be provided for by the Unit or the respective Security Market Player, from time to time;

j) where the transaction is carried out in a single operation or several operations that appear to be linked;

k) carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between Securities Market Players and when credit or debit cards are used as a payment system to effect money transfer;

l) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in this guideline; and

m) there are doubts about the veracity or adequacy of previously obtained customers identification data.

2.1.4 SMPs shall not be permitted to keep anonymous accounts or accounts in fictitious names.

2.1.5 Where nominee accounts are maintained, details of the beneficial owners shall be provided on request.

2.1.6 **Shell banks**: - These are banks which have no physical presence in any jurisdiction. Shell banks are prohibited from operating in Zimbabwe.

2.1.6.1 SMPs are not allowed to establish correspondent relationships with shell banks and high risk foreign banks, or correspondent banks that permit their accounts to be used by such banks.

2.1.6.2 SMPs shall take all necessary measures to satisfy themselves that correspondent Securities Market Players in a foreign country do not permit their accounts to be used by shell banks.

Cancellation & Cooling-Off Rights

2.1.7 Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid subject to some deductions, where applicable.

2.1.7.1 Since cancellation/cooling-off rights could offer a readily available route for laundering money, Securities Market Players shall be alert to any abnormal exercise of these rights by an investor.

2.1.7.2 In the event where abnormal exercise of these rights becomes apparent, the matter shall be treated as suspicious and reported to the FIU.

2.2 CDD Requirements for Securities Market Players

2.2.1 A Securities Market Player shall;

b) identify and verify the identity of every customer and beneficial owner,

c) obtain information on the purpose and intended nature of the business relationship, and

d) conduct ongoing due diligence for customers that the designated institution has an account with or has established a business relationship with.

2.2.2 SMPs are required to obtain, verify and maintain accurate and meaningful information (name, address and account number) on all investments.

Simplified/Reduced CDD

2.2.3 A designated institution is allowed to apply reduced or simplified identification measures where the risk of money laundering or terrorist financing is lower. The measures shall be documented and must be approved by the board.

2.2.3.1 There are low risks in circumstances where;

a) Information on the identity of the customers and the beneficial owner of a customer is publicly available.

b) Adequate checks and controls exist elsewhere in national systems.

2.2.3.2 The following may be considered to be low risk customers:

a) Public companies (listed on a Stock Exchange or similar situations) that are subject to regulatory disclosure requirements;

b) Government ministries and parastatals/enterprises;

c) Beneficial owners of pooled accounts held by Designated Non-Financial Businesses and Professions (DNFBPs), provided that they are subject to AML/CFT requirements consistent with the provisions of the BUPSML Act.

2.2.4 Other alternative methods of verifying residential addresses of low risk individuals that may be considered acceptable to an SMP, include;

a) Letters from employers,

b) Affidavits from landlords,

c) Third party home owner certificates,

d) Letters from schools, chiefs and head men,

e) Referral letters from senior bank officials,

f) Letter from a practicing accountant,

g) Letter from existing bank customer,

h) Letter from a practicing doctor,

i) Letter from a practicing lawyer,

j) Letter from a Government arm.

2.2.5 In addition, information beyond customer identity, such as customer location and purpose of the transaction, is needed to adequately assess risk. This will be an iterative process. The preliminary information obtained about a customer should be sufficient to determine whether to proceed with establishing the business relationship.

Enhanced Due Diligence

2.2.6 An SMP shall apply enhanced due diligence measures based on risk assessment. For higher risk customers, intensive due diligence shall be required, especially for those whose source of funds are not clear.

2.2.7 Examples of customers requiring enhanced due diligence include;

a) Non-resident customers;
b) customers from countries that do not or insufficiently apply the FATF standards;
c) high net worth individuals;
d) politically exposed persons (PEPs);
e) non-face-to-face customers;
f) customers with dubious reputation as per public information available;
g) transactions involving accounts in multiple jurisdictions;
h) the use of front persons or entities (e.g. corporations, trusts);
i) entities with complex corporate structures;
j) unregistered or unregulated investment vehicles; and
k) cross-border omnibus and correspondent accounts.

2.2.8 Upon determining customers as high-risk, the reporting Securities Market Player shall undertake enhanced CDD process on the customers, which shall include enquiries on:

a) the purpose for opening an account;
b) the level and nature of trading activities intended;
c) the ultimate beneficial owners;
d) the source of funds;
e) senior management's approval for opening the account /s of corporate.

2.3 KYC Policy

2.3.1 Know Your Customer is that part of customer due diligence procedures that SMPs and other regulated companies must perform to identify their clients and ascertain relevant information pertinent to doing financial business with them.

2.3.2 Securities Market Players should put in place KYC policies and procedures which incorporate the following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and

d) Risk Management.

2.3.3 **Customer Acceptance Policy (CAP)**

2.3.3.1 Every SMP shall develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that guidelines are in place on the following aspects of customer relationship with the designated institution.

a) No transaction shall be conducted in anonymous or fictitious name(s). SMPs shall not allow any transaction in any anonymous or fictitious name (s) or on behalf of other persons whose identity has not been disclosed or cannot be verified.

b) A designated institution shall not conduct any transaction where it is unable to apply appropriate customer due diligence measures i.e. the designated institution is unable to verify the identity and /or obtain documents required due to non-cooperation by the customer or non reliability of the data/information furnished to the designated institution.

2.3.3.2 Circumstances in which a customer is permitted to act on behalf of another person/entity shall be clearly spelt out. The beneficial owner shall be identified and all reasonable steps taken to verify his identity.

2.3.3.3 SMPs shall prepare a profile for each new customer, where regular transactions or a continuing business relationship is expected, based on risk categorisation. The customer profile may contain information relating to customer's identity, social / financial status, etc.

2.3.3.4 The nature and extent of due diligence will depend on the risk perceived by the designated institution. However, while preparing customer profile, SMPs should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive.

2.3.3.5 SMPs should note that customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

2.3.4 **Customer Identification Procedure**

2.3.4.1 Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. A designated institution shall obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional.

2.3.4.2 Being satisfied means that the designated institution must be able to satisfy the competent authorities that due diligence was observed.

2.3.4.3 For customers that are natural persons, the designated institution shall obtain sufficient identification document/s to verify the identity of the customer such as;

(i) National identity document,
(ii) Valid Passport,
(iii) Driving licence and
(iv) Letter from a recognized public authority or public servant verifying the identity of the customer to the satisfaction of the designated institution.

2.3.4.4 For customers that are legal persons (corporates, clubs, societies and charities and legal arrangements), the designated institution shall establish the following;

(i) name of company;
(ii) the legal status of the legal person through proper and relevant documents;
(iii) the identities of the directors, and their proof of residence;
(iv) any person purporting to act on behalf of the legal person must be authorized and identified. His identity must be verified;
(v) the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person (Beneficial owner(s);
(vi) principal place of company's business operations;
(vii) mailing address of company and contact numbers;
(viii) tax clearance certificate;

(ix) the original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;

(x) board of Directors resolution to invest, and identification of those who have authority to operate the investment account;

(xi) nature and purpose of business and its legitimacy.

2.3.4.5 The designated institution shall introduce a system of periodical updating of customer identification data, if there is a continuing business relationship.

2.3.4.6 When there are suspicions of money laundering or financing of terrorism, or where there are doubts about the adequacy or veracity of previously obtained customer identification data, the designated institution shall review the due diligence measures including verifying again the identity of the customer and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

Non Face-to-Face Identification

2.3.4.7 In view of possible false identities and impersonations that may arise with non face-to-face customers, additional measures/checks shall be undertaken to supplement the documentary or electronic evidence.

2.3.4.8 These additional measures/checks will apply whether the applicant is resident in Zimbabwe or elsewhere, and shall be particularly robust where the applicant is requiring a product/service that offers money transmission or third party payments.

2.3.4.9 Procedures to identify and authenticate the customer shall be put in place to ensure that there is sufficient evidence either documentary, or electronic to confirm his address and personal identity, and to undertake at least one additional check to guard against impersonation and fraud.

2.3.4.10 If reliance is being placed on intermediaries to undertake the processing of applications on the customer's behalf, checks shall be undertaken to ensure that the intermediaries are regulated for ML/FT prevention, and that the relevant identification procedures are applied. In all cases, evidence as to

how identity has been verified shall be obtained and retained with the customer records.

2.3.4.11 SMPs shall conduct regular monitoring of internet-based business/customers. If a significant proportion of the business is operated electronically, computerised monitoring systems/solutions that are designed to recognise unusual transactions and related patterns of transactions shall be put in place to recognise suspicious transactions.

2.3.4.12 The MLRO is required to review these solutions, record exemptions and report same, to the FIU.

Trust, Nominees and Fiduciaries

2.3.4.13 Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of criminal funds they wish to launder.

2.3.4.14 Identification procedures shall be set and managed according to the perceived risks in trusts, nominees and fiduciaries accounts.

2.3.4.15 Securities Market Players shall obtain and verify the identity of those providing funds for the Trust.

2.3.4.16 The principal objective for ML/FT prevention via trusts, nominees and fiduciaries is to verify the identity of the provider of funds such as the settlor, those who have control over the funds (the trustees), and any controller who have the power to remove the trustees.

2.3.4.17 For discretionary or offshore trusts, the nature and purpose of the trust and the original source of funding must be ascertained.

2.3.4.18 Identification requirements must be obtained and not waived for any trustee who does not have authority to operate an account, and cannot give relevant instructions concerning the use or transfer of funds.

Offshore Trusts

2.3.4.19 Offshore Trusts present a higher ML/FT risk and therefore additional identification measures are needed for Special Purpose Vehicles (SPVs) or

Multinational companies connected to Trusts, particularly when Trusts are set up in offshore locations, with strict bank secrecy or confidentiality rules.

2.3.4.20 Those created in jurisdictions without equivalent AML/CFT procedures in place shall warrant additional enquiries.

2.3.4.21 Unless that customer is a regulated Securities Market Player, measures shall be taken to identify the Trust company, or the corporate service provider, in line with the requirements for companies.

2.3.4.22 For overseas Trusts, nominee and fiduciary accounts, where the customer is itself a Securities Market Player that is regulated for ML/FT purposes:

a) reliance can be placed on an introduction or intermediary certificate letter, stating that evidence of identity exists for all underlying principals and confirming that there are no anonymous principals;

b) the trustees/nominees shall be asked to state from the outset the capacity in which they are operating or making the application;

c) documentary evidence of the appointment of the current Trustees shall also be obtained.

2.3.4.23 Any application to open an account or undertake a transaction on behalf of another without the customer identifying their Trust or Nominee capacity, shall be regarded as suspicious and shall lead to further enquiries and submission of reports to the FIU.

Additional CDD Requirements for Politically Exposed Persons (PEPs)

2.3.4.24 Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a local or foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, political party officials, etc.

2.3.4.25 A designated institution shall gather sufficient information on any person/customer of this category intending to undertake a transaction and check all the information available on the person in the public domain.

2.3.4.26 It should apply enhanced customer due diligence when verifying the identity of the PEP and must seek information about the source/s of wealth and source/s of funds before accepting the PEP as a customer.

2.3.4.27 The decision to undertake a transaction with a PEP shall be taken at a senior level, which shall be clearly spelt out in the Customer Acceptance Policy. They should also subject such transactions to enhanced monitoring on an ongoing basis.

2.3.4.28 The above requirements may also be applied to transactions with family members or close relatives of PEPs. The requirements may also be applied to customers who become PEPs subsequent to establishment of the business relationship.

2.3.4.29 These requirements are also applicable to transactions where a PEP is the ultimate beneficial owner.

2.3.4.30 Furthermore, in relation to transactions involving PEPs, it is reiterated that a designated institution shall have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, family members or close relatives of PEPs and transactions of which a PEP is the ultimate beneficial owner.

Correspondent Relationship/ Foreign Securities Market Players

2.3.4.31 When dealing with Correspondent Relationship/Foreign Securities Market Players, SMPs are required to confirm the existence and regulated status of such institutions using the following means:

i. checking with the home country's Securities Market Regulator or relevant supervisory body;
ii. checking with another office, subsidiary or branch in the same country;
iii. checking with the Zimbabwean regulated correspondent Securities Market Player of the overseas Player;
iv. obtaining evidence of its licence or authorization to conduct Securities business from the Player itself.

2.3.4.32 Transactions conducted through correspondent relationships need to be managed using a risk-based approach.

2.3.4.33 KYC procedures in relation to correspondents are required to be established to ascertain whether or not the correspondents Securities Market Player, or the counter-party, is regulated for ML/TF prevention.

2.3.4.34 Securities Market Players shall guard against establishing correspondent relationships with high-risk foreign banks (e.g. **shell banks** with no physical presence in any country), or with correspondent banks that permit their accounts to be used by such banks.

Introduced Business

2.3.4.35 SMPs are permitted to rely on introduced business. In respect of group introducers from outside Zimbabwe, arrangements shall be put in place to ensure that identity is verified in accordance with requirements and that the underlying records of identity in respect of introduced customers are retained for the prescribed period.

2.3.4.36 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that:

i. the identity of the customers has been verified by the introducing parent company, branch, subsidiary or associate in line with the AML/CFT requirements of equivalent standards and taking account of any specific requirements;

ii. no exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship;

iii. a group introduction letter is obtained and placed with the customers' account opening records.

2.3.4.37 Securities Market Players shall ensure that there is no secrecy or data protection legislation with the introducers, which would restrict free access to the records on request by the FIU, or by law enforcement agencies under court order, or relevant mutual assistance procedures.

CDD on Existing Customers

2.3.4.38 Securities Market Players shall apply CDD requirements to existing customers on the basis of materiality and risk, and shall continue to conduct due diligence on all existing relationships at appropriate times.

On-going CDD

2.3.4.39 Securities Market Players shall conduct on-going CDD when:

a) there is suspicion of ML/TF,
b) a transaction of significant value takes place,
c) customer documentation standards change substantially,
d) there is a material change in the way that the account is being operated,
e) the institution becomes aware that it lacks sufficient information about an existing customer.

2.3.5 Monitoring of Transactions

2.3.5.1 Designated Institutions are expected to have an understanding of the normal transacting patterns and source of funds of their customer. This will give the designated institution the means to identify transactions that fall outside the regular pattern of activity.

2.3.5.2 However, the extent of monitoring will depend on the risk sensitivity of the transaction. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

2.3.5.3 Each SMP may prescribe limits for a particular category of transaction and pay particular attention to the receipts which exceed these limits. High-risk receipts have to be subjected to intense monitoring.

2.3.5.4 A SMP shall set key indicators for such receipts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

2.3.5.5 A SMP shall put in place a system of periodical review of risk categorization of customers and the need for applying enhanced due diligence measures.

2.3.5.6 Designated institutions shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in the FATF Statements and countries that do not or insufficiently apply the FATF Recommendations.

2.3.5.7 In addition, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents retained and made available to the FIU and other relevant authorities, on request.

2.3.5.8 Where a designated institution is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the designated institution shall not undertake the transaction.

2.3.5.9 In the case of existing business relationship, the SMP shall terminate such business relationship if the customer fails to comply with the customer due diligence requirements. Under these circumstances, designated institution shall make a suspicious transactions report to the FIU in relation to the customer, even if the transaction did not go through (attempted transaction).

2.3.6 **Risk Management**

2.3.6.1 Risk analysis must be performed, and kept up to date, to determine where money laundering and terrorist financing risks are greatest.

2.3.6.2 Designated institutions need to identify the main vulnerabilities and address them accordingly.

2.3.6.3 Higher risk customers, products and services, including delivery channels, and geographical locations should be identified.

2.3.6.4 Risk assessment must include a variety of factors, depending upon particular circumstances, including but not limited to:

a) The nature, scale and complexity of the customer's operations, including geographical diversity;
b) The initial and ongoing due diligence or monitoring conducted on the customer;
c) Any previous relationships with the applicant or other parties to the application;
d) Time scale, especially in relation to early encashment (whether for the current application or previous investments) ;
e) The designated institution's customer, product, and activity profile;
f) The nature of the business relationship (*i.e.* occasional vs. ongoing relationship) ;
g) The volume and size of investments/transactions ;
h) The extent to which the designated institution is dealing directly with customers or is dealing through intermediaries, third parties or in a non-face-to-face setting.

2.3.6.5 To conduct a proper risk-based approach, designated institutions need to collect information relevant to its operations.

2.3.6.6 The effectiveness of the risk-based approach would increase significantly if SMPs are able to share information with other relevant institutions, including foreign counterparts.

Controls for Higher Risk Situations

2.3.6.7 A SMP shall implement appropriate measures and controls to mitigate the potential ML/TF risks for situations that are considered to be of higher risk as a result of the designated institution's risk assessment.

2.3.6.8 These measures and controls may include:

a) Increased levels of KYC or enhanced due diligence, such as proactive contact with the customer to determine the reason for the transactions and the source of funds.

b) Increased levels of controls and frequency of reviews of customer relationships.
c) Increased transaction monitoring of higher-risk products, services and channels.
d) Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent location.

2.3.6.9 The same measures and controls may often address more than one of the risk criteria identified.

2.3.6.10 Designated institutions should pay special attention to any money laundering/terrorist financing threats that may arise from new or developing technologies, including transactions through internet, which might favour anonymity.

Implementation of Risk-Based Approach to AML/CFT Programmes

2.3.6.11 SMPs shall formulate and implement a risk-based approach to their AML/CFT programmes.

2.3.6.12 This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures.

2.3.6.13 This should be evidenced by categorisation of the customer base, products and services by risk rating (e.g. low, medium, and high) and identification of assigned actions by risk types.

2.3.6.14 Whilst each designated institution will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks.

2.3.6.15 A SMP shall conduct periodic reviews (not more than two years apart) to determine whether any adjustment should be made to the risk rating.

2.3.6.16 The review of the risk rating for high risk customers may be undertaken more frequently than for other customers. Senior management shall then determine whether the business relationship should be continued or stopped.

2.3.6.17 All decisions regarding high risk relationships and the basis for these decisions shall be documented.

2.3.6.18 The risk rating framework should take into account customer acceptance and on-going monitoring policies and procedures that assist the designated institution in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk.

2.3.6.19 A more extensive customer due diligence process should be adopted for higher risk customers. There shall also be a clear internal guideline on which level of management that is able to approve business relationships with such customers.

2.3.6.20 The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason/s for such changes.

2.3.6.21 A designated institution shall therefore design an AML/CFT framework that satisfies the needs of its institution, but should include at a minimum:

a) Differentiation of customer relationships by risk categories (such as high, moderate or low);
b) Differentiation of customer relationships by risk factors (such as products, customer type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size, volume and type of transactions, cash transactions, adherence to customer activity profile);
c) KYC documentation and due diligence information requirements appropriate for each risk category and risk factor; and
d) Requirements for the approval of upgrading and downgrading of customer risk ratings.

2.3.6.22 SMPs shall establish a customer's profile, taking into account, at a minimum:

a) The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);
b) The complexity, volume and pattern of transactions;
c) Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports transaction patterns, whether customer is known to other members of the

financial group, whether delegated authority such as power of attorney is in place);

d) Delivery channels (e.g. mobile/internet banking, wire transfers to third parties);
e) Geographical origin of the customer;
f) Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);
g) Whether the origin of wealth and/or source of funds can easily be verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
h) Unwillingness of the customer to co-operate with the designated institution's customer due diligence process for no apparent reason;
i) Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

2.3.6.23 Accordingly, an SMP may apply customer due diligence standards on a risk sensitive basis, consistent with these Guidelines, depending on the type of customer, business relationship or transaction.

2.3.6.24 Reduced due diligence is acceptable in cases where the risk of ML/TF is low, for example where information on the identity of the customer or beneficial owner is publicly available.

2.3.6.25 Alternatively, a designated institution shall apply enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high. It follows then, that simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or where specific higher risk scenarios apply.

2.3.6.26 In addition to examples of suspicious transactions appended to this Guideline, typologies of money laundering and terrorist financing schemes are available at websites such as www.fatf-gafi.org.

2.3.6.27 An SMP shall ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories, and that the requisite due diligence is being followed.

2.3.6.28 In addition, an SMP shall periodically review their risk categories as typologies evolve on practices by money launderers and terrorists. These reviews shall not be undertaken more than two years apart.

3 INTERNAL CONTROLS, POLICIES & PROCEDURES

3.1 General

3.1.1.1 The Board of Directors of an SMP shall ensure that effective internal controls are put in place, by establishing appropriate AML/CFT policies and procedures, and ensuring effective implementation.

3.1.1.2 The ultimate responsibility for AML/CFT compliance is placed on the Board/Top Management of every SMP.

3.1.1.3 The Board shall ensure that a comprehensive operational AML/CFT Policy Manual is formulated by Management and presented to the Board for consideration and formal approval.

3.1.1.4 The internal controls, policies and procedures shall cover proper management oversight systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the SMP so as to ensure that the policies and procedures are implemented effectively.

3.1.1.5 A designated institution's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the AML/CFT policies and procedures.

3.1.1.6 As a general rule, the compliance function should provide an independent evaluation of the SMP's own policies and procedures, including legal and regulatory requirements.

3.1.1.7 A designated institution shall ensure that its audit machinery is staffed adequately with individuals who are well-versed with such AML/CFT policies and procedures.

3.2 Appointment Of A Money Laundering Reporting Officer (MLRO)

3.2.1 An SMP shall appoint a senior management officer as Money Laundering Reporting Officer (MLRO). The MLRO shall be located at the head/corporate office of the designated institution.

3.2.2 The MLRO shall, among other things, be responsible for;

a) Monitoring and reporting of all suspicious transactions and sharing of information as required under the BUP&SML Act and the guidelines,

b) Overseeing and ensuring overall compliance with regulatory guidelines on AML/ CFT issues from time to time,

c) Developing appropriate compliance management arrangements across the full range of AML/CFT areas (e.g. CDD, record keeping, etc.),

d) Maintaining close liaison with law enforcement agencies, other designated institutions and any other institutions, which are involved in the fight against money laundering and combating financing of terrorism.

3.2.3 To enable the MLRO to discharge his responsibilities, a designated institution shall ensure that the MLRO and other appropriate staff members have timeless access to customer identification data and other CDD information, transaction records and other relevant information.

3.2.4 Furthermore, a designated institution shall ensure that the MLRO is able to act independently and report directly to senior management or to the Board of Directors.

Recommended Procedures

3.2.5 Every SMP operating within Zimbabwe shall:

a) Have procedures for the prompt validation of suspicious transaction and subsequent reporting by the internal employees to the MLRO.

b) Provide the MLRO with the necessary access to systems and records to enable him/her to investigate and validate internal suspicious reports which would have been reported to him.

c) Inform all employees of the identity of the MLRO and in his absence, the alternative MLRO.

4 REPORTING OF SUSPICIOUS TRANSACTIONS

4.1 The Bank Use Promotion and Suppression of Money Laundering Act (Chapter 24.24), imposes obligations on designated institutions to report suspicious transactions to the Unit**.**

4.2 While determining suspicious transactions, a SMP shall be guided by the definition of a suspicious transaction as stated in the definition of terms table.

4.3 A designated institution shall write and submit a STR to the FIU, if it has reasonable ground of believing that the transaction, including an attempted transaction, involves proceeds of crime, irrespective of the amount of transaction and/or the limit envisaged for predicate offences as defined by the Serious Offences Act.

4.4 The Suspicious Transaction Report shall be furnished to the Unit within 3 days after determination that the transaction is suspicious.

4.5 The MLRO shall record his reasons for treating any transaction or a series of transactions as suspicious. The SMP shall ensure that there is no undue delay in arriving at such a conclusion once a suspicious transaction activity has been identified. An STR shall then be filed with the FIU.

4.6 It is likely that in some cases, transactions are abandoned/aborted by customers on being asked to give more details or to provide documents.

4.7 In such cases, a designated institution shall report all such attempted transactions by means of an STR, even if the transaction was not completed by the customer, and irrespective of the amount involved.

4.8 When reporting an STR, a SMP shall use STR Template provided as **Annexure 1**.

4.9 In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, SMPs may consider the following indicative list of suspicious activities.

Examples of Transactions That May Trigger Suspicion

a) Transaction where one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another.
b) A customer's transactions include a pattern of sustained losses.
c) The purchase and sale of non-listed securities with a large price differential within a short period of time.
d) Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without identifying who they are for or providing very little information regarding the underlying account holder or beneficiary.
e) A company uses cash to pay dividends to investors.
f) Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.
g) Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.
h) A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).
i) A customer's transactions have no apparent economic purpose.
j) Changing share ownership in order to transfer wealth across borders;
k) Opening multiple accounts or nominee accounts;
l) Using brokerage accounts as long term depository accounts for funds;

m) Effecting transactions involving nominees or third parties;

n) Engaging in market manipulation, e.g. “pump & dump” schemes;

o) A customer who is unfamiliar with a financial product’s performance and specifications but wants to invest in it nonetheless.

p) Transactions that show the customer is acting on behalf of third parties.

q) The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.

r) Transactions involving an unknown counterparty.

s) Large cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

NB: The above list is only indicative and not exhaustive.

Confidentiality and Tipping-off

4.10 SMPs shall not put any restrictions on payment to beneficiaries where a STR has been made. Moreover, a designated institution shall ensure that employees keep the fact of furnishing such information as strictly confidential, and there is no **tipping-off** to the customer at any level.

5 MAINTENANCE OF RECORDS OF TRANSACTIONS

5.1 The Bank Use Promotion and Suppression of Money Laundering Act (Chapter 24.24), imposes obligations on designated institutions to record and maintain customer information and transactions.

5.2 An SMP shall operate within the provisions of the Act, and shall take all steps considered necessary to ensure compliance with the requirements of the Act. It shall introduce a system of maintaining proper record of transactions prescribed under this requirement.

5.3 Information maintained in respect of transactions shall permit reconstruction of individual transactions, and if necessary, evidence for prosecution of persons involved in criminal activities.

5.4 Some of the customer and transactions information to be recorded and maintained include the following:

a) identity of the customer;
b) the type and nature of the transaction;
c) the amount of the transaction and the currency in which it was denominated;
d) date of transaction; and
e) the parties to the transaction.

5.5 SMPs shall take appropriate steps to evolve and maintain a system that allows data to be retrieved easily and quickly whenever required, or when requested by competent authorities.

5.6 The records shall be kept for at least **five years** from the date of transaction, between the designated institution and the customer.

6 CUSTOMER EDUCATION and EMPLOYEES' TRAINING

6.1 Customer Education

6.1.1 Implementation of KYC procedures requires SMPs to demand certain information from a customer that may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information.

6.1.2 There is, therefore, a need for a designated institution to prepare specific literature/ pamphlets, etc. which shall educate the customer of the objectives of the KYC programme.

6.1.3 Front office staff needs to be specially trained to handle such situations while dealing with customers.

6.2 Employees' Training

6.2.1 Financial institutions are required to design comprehensive employee education and training programs not only to make employees fully aware of their obligations, but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks. The establishment of such an employee training program is not only considered as best practice but a statutory requirement.

6.2.2 An SMP shall conduct an ongoing employee training programme which ensures that members of staff are adequately trained so that they are aware of :-

a) policies and procedures relating to prevention of money laundering and counter terrorist financing, and
b) the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of transactions.

6.2.3 The timing, coverage and content of the employee training program shall be tailored to meet the perceived needs of the SMP and in line with AML/CFT legislations.

6.2.4 A comprehensive training program is required to encompass staff/areas such as Compliance officers; new staff (as part of the orientation program for those posted to the front office); branch office staff (particularly cashiers, account opening mandate, and marketing staff); internal control/audit staff and managers.

6.2.5 It is crucial that all staff members responsible for combating ML and TF fully understand the rationale behind the AML/CFT policies, and the need for them to implement such policies consistently.

6.2.6 SMPs shall keep a record of all AML/CFT training materials delivered to its employees.

6.2.7 The steps to be taken when staff members come across any suspicious transaction (such as asking questions about the source of funds, checking the identification documents carefully, reporting immediately to the MLRO etc.)

should be carefully and clearly formulated by the SMP, and the respective procedure properly laid down in the SMP's internal AML/CFT policy document.

6.2.8 Financial institutions are required to inform their employees in writing, to make such reports confidential and that they will be protected from victimization for making them.

6.2.9 SMPs are required to review their AML/CFT framework from time to time with a view of determining their adequacy and identifying other areas of potential risks not covered by the AML/CFT Compliance Manual

---