Bank Use Promotion and Suppression of Money Laundering Unit

GUIDELINES ON ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM FOR MONEY TRANSFER AGENCIES & BUREAUX DE CHANGE, 2012

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

These guidelines amplify and explain the statutory obligations that Money Transfer Agencies (MTAs) and Bureaux de Change 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, laying down minimum standards on Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) measures for MTAs and Bureaux de Change.

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 own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also covers those persons who exercise ultimate effective control over a legal person or arrangement.
BdC	Bureau de Change
BUPSML UNIT / FIU or Unit	Refers to the Bank Use Promotion and Financial Intelligence Unit established in terms of the Bank Use Promotion and Suppression of Money Laundering Act
BUPSML Act	Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24]
BUPSML Unit	Bank Use Promotion and Suppression of Money Laundering Unit established in terms of the Bank Use Promotion and Suppression of Money Laundering Act (otherwise known as "the Financial Intelligence Unit or "FIU")
Business relationship	Means any arrangement between the financial 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.
CDD	Customer Due Diligence
Designated Institution	Means any institution designated in terms of the Bank Use Promotion and Suppression of Money Laundering Act for purposes of implementing statutory AML / CFT obligations prescribed therein and includes an individual or entity carrying on the business of a Money Transfer Agency or a Bureau de Change
DNFBPs	Designated Non Financial Businesses and Professions
FIU	Financial Intelligence Unit (referred to in the Act as the Bank Use Promotion and Suppression of Money Laundering Unit.
KYC	Know Your Customer principle
MTA	Money Transfer Agency
PEP	Politically Exposed Person. This refers to a person holding high public office and includes spouse, close relative or associate of such person.
STR	Means Suspicious Transaction Report and includes an attempted transaction
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.

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 them 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, the Bank Use Promotion and Financial Intelligence Unit (hereinafter referred to as the "BUPSML UNIT" or simply "the Unit") 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.

1.2 ***What is Money Laundering and Terrorist Financing?***

1.2.1 Money Laundering is any transaction that is designed to disguise the illegal source of proceeds of crime in order to make it look like the funds came from a legitimate source.

1.2.2 There are various methods of laundering proceeds of crime, including transmitting such funds through the formal financial systems 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 every offence defined as "serious offence" in terms of the Serious Offences (Confiscation of Profits) Act. Such offences 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 Criminals favour using financial systems of countries to clean up and disguise the illicit origins of proceeds of their crimes. 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.

1.2.8 Zimbabwe, like most other countries of the world, has put in place legislative and other measures 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.

1.2.9 It is in this context that the law requires designated institutions to implement AML/CFT measures, including submitting Suspicious Transaction Reports (STRs) to the national Financial Intelligence Unit.

1.2.10 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.

1.2.11 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. The Act also establishes the Bank Use Promotion and Suppression of Money Laundering Unit (BUPSML Unit), which is a Unit within the Reserve Bank of Zimbabwe tasked with overseeing compliance with the Act.

1.3 *The Role of the BUPSML Unit*

1.3.1 The main statutory function of the BUPSML Unit is to enforce compliance

1.3.2 The BUPSML UNIT is the Financial Intelligence Unit of the country responsible for enforcing compliance with AML / CFT legislation and Guidelines by designated reporting institutions.

1.3.3 More particularly, the BUPSML Unit is responsible for –

- Receiving STRs from designated institutions;
- Analyzing the received STRs;
- Disseminating STRs of interest to law enforcement agencies;
- Supervising and monitoring designated institutions to ensure compliance with the Act and AML/CFT Guidelines.

1.4 ***What are Designated Institutions?***

1.4.1 Designated institutions are those institutions designated by the BUPSML Act for purposes of complying with the AML/CFT requirements prescribed under the Act such as submission of STRs and putting in place other specified AML / CFT measures. The list of designated institutions includes Financial Institutions and Designated Non Financial Businesses and Professions (DFNBPs).

1.4.2 The list of Designated Institutions includes Banks; insurance companies; legal practitioners; public accountants; estate agents, moneylenders, pension funds; asset managers; bureau de change and money transfer agencies.

1.4.3 For the purposes of this Guideline, Designated Institutions refers to Money Transfer Agencies (MTAs) and Bureaux de Change (BdC).

1.5 ***MTAs and Bureaux de Change***

1.5.1 MTAs refer to institutions that offer the money or value transfer

1.5.2 BdC refer to institutions that offer the following services to the public: buying or selling foreign currency or exchanging one currency for another through the application of exchange rates.

1.5.3 The same institution may be licenced to carry out both MTA and BDC services.

1.5.4 While an MTA or a BdC must be licenced / registered in order to operate lawfully, the fact that an institution or individual offers MTA or BdC services, whether occasionally or on an ongoing basis, while not being registered does not exempt such individual or entity from complying with the BUPSML Act or these Guidelines.

1.5.5 MTAs operate in a variety of ways, but typically involve a sending agent which accepts payment of money transfer, collects the required identification information, and systematically enters the transaction and sender's applicable identification information and that of the intended receiver at the point of origination.

1.5.6 The funds are made available to the ultimate recipient, in the appropriate currency, at a receiving agent location in the paying jurisdiction.

1.5.7 MTAs can easily be used by criminals to launder proceeds of crime or to channel funds destined to fund terrorist activities.

1.5.8 MTAs provide a conduit for dirty funds to be cleansed and to be moved away from their source of origin.

1.5.9 In some cases, MTAs and BdC maintain accounts or ongoing business relationships with certain customers while in many cases MTAs also transact with walk-in clients on occasional or once-off basis.

1.5.10 The BUPSML Act and these Guidelines seek to ensure that MTAs put measures in place to deter as well as detect transactions that involve or are suspected to involve money laundering and financing of terrorism.

1.5.11 MTAs and BdC should develop suitable mechanisms for enhanced monitoring of transactions suspected of having terrorist and/or money laundering links.

2 CUSTOMER DUE DILIGENCE & KNOW YOUR CUSTOMER 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.

2.1.2 CDD procedures enable designated institutions to know/understand their customers and their financial dealings better, which in turn helps to identify unusual or suspicious transactions and to manage risks prudently.

2.2 Definition of Customer

2.2.1 In relation to MTAs, a ‘Customer’ is defined as:

- a person who receives occasional/ regular local or cross border inward remittances using a money transfer agency

- one on whose behalf a local or cross border inward remittance under MTAs is received (i.e. the beneficial owner)

2.2.2 In relation to BdC, a 'Customer' is a person who exchanges, buys, or sells foreign currency.

2.3 CDD Requirements for Designated Institutions

2.3.1 Designated institutions shall not be allowed to keep anonymous accounts or accounts in obviously fictitious names.

2.3.2 Designated institutions shall be required to undertake customer due diligence (CDD) measures when:

- establishing business relations;
- carrying out occasional transactions above the applicable designated threshold or wire transfers transactions
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

2.3.3 A designated institution shall:

- Identify the customer and verify that customer's identity using reliable, independent source documents, data or information
- Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, designated institutions should understand the ownership and control structure of the customer
- obtain information on the purpose and intended nature of the business relationship; and

- conduct ongoing due diligence for customers that the designated institution has an account with or has established a business relationship with;
- apply enhanced CDD measures –

    - where there are doubts regarding the accuracy or veracity of previously obtained information; or
    - where the designated institution has identified a particular customer or transaction as representing a high money laundering or terrorist financing risk.
    - in the transaction involves a PEPs; or
    - where there is suspicion of money laundering; or

2.3.4 For cross-border transactions, MTAs are required to obtain and maintain accurate and meaningful information of;

- the name of the originator;
- the originator account number where such an account is used to process the transaction;
- the originator's address, or national identity number, or customer identification number, or date and place of birth;
- the name of the beneficiary; and
- the beneficiary account number where such an account is used to process the transaction.

2.3.5 The information should remain with the transfer or related messages through the payment chain.

2.3.6 For domestic wire transfers, however, the ordering MTA may include full originator information or only the originator's account number or unique identifier; provided full originator information is available to the recipient MTA and competent authorities within three (3) business days.

2.3.7 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 should be documented and must be approved by the board.

2.3.8 Where the simplified CDD measures are subject to certain conditions being met, it is necessary to verify that these conditions apply, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. In addition, information beyond customer identity, such as customer location and purpose of the transaction, may be 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 go further, and in many cases customer monitoring will provide additional information.

2.4 KYC Principle

2.4.1 Designated Institutions should put in place KYC policies and procedures which incorporate the following four key elements:

- Customer Acceptance Policy;
- Customer Identification Procedures;
- Monitoring of Transactions; and
- Risk Management.

2.4.2 *Customer Acceptance Policy*

2.4.2.1 Every designated institution shall develop a clear customer acceptance policy laying down explicit criteria for acceptance of customers. The customer acceptance policy shall ensure that explicit guidelines are in place on the following aspects of customer relationships with the designated institutions:

- No transaction shall be conducted in anonymous or fictitious name(s). Designated Institutions shall not allow any account or transaction in an anonymous or fictitious name or on behalf of a person whose identity has not been disclosed or cannot be verified.
- A designated institution shall not conduct any transaction where it is unable to apply appropriate CDD measures i.e. the designated institution

is unable to verify the identity and /or obtain documents required due to non-cooperation of the customer or non reliability of the data/information furnished to the designated institution.

2.4.2.2 Circumstances in which a customer is permitted to act on behalf of another person/entity shall be clearly spelt out and supporting documents should be furnished showing that the person is authorized to act on behalf of another (natural or legal) person. The beneficial owner should be identified and all reasonable steps should be taken to verify his identity.

2.4.2.3 The designated institution shall prepare a profile for each new customer, where regular transactions or a continuing business relationship is expected, based on risk categorization. The customer profile may include information relating to customer's identity, social / financial status, etc.

2.4.2.4 The nature and extent of due diligence will depend on the risk perceived by the designated institution. However, while preparing a customer profile, a designated institution is required to take care to seek only such information from the customer, as shall be relevant to the risk category and is not intrusive.

2.4.2.5 A designated institution shall apply enhanced due diligence measures based on risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the source of funds are not clear. Examples of customers requiring enhanced due diligence include:

- nonresident customers;
- customers from countries that do not or insufficiently apply the FATF standards;
- high net worth individuals;
- politically exposed persons (PEPs);
- non-face to face customers; and
- those with dubious reputation as per public information available, etc.

2.4.2.6 An MTA shall, before making a payment, carry out enhanced CDD whenever there is suspicion of money laundering or terrorist financing, or when other

factors give rise to a belief that the customer or particular transaction poses a high risk,.

2.4.3 **Customer Identification Procedures**

2.4.3.1 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.

2.4.3.2 The designated institution must be able to satisfy the Unit that due diligence was observed.

2.4.3.3 For customers that are natural persons, the designated institution shall obtain sufficient identification document/s to verify the identity of the customer, such as a national identity document, valid passport or valid driver's licence.

2.4.3.4 For customers that are legal persons, the designated institution shall;

(i) verify the legal status of the legal person through proper and relevant official documents, such as documents from the Company Registry office;

(ii) verify that any person purporting to act on behalf of the legal person is so authorized and identify and verify the identity of that person. For those customers who are legal persons e.g. companies, clubs, societies and charities and legal arrangements, the Designated Institution shall obtain a letter of authorization, resolution or other acceptable and legally valid document from the entity showing that the person acting on behalf of the legal person or entity is properly authorised to so act and conduct transactions on behalf of the entity;

(iii) understand the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person/ beneficial owner(s).

2.4.3.5 Any natural person conducting the transaction on behalf of a legal person or entity shall be subjected to the same identification requirements as applied to a customer who is a natural person, i.e. identification documents of that person shall be obtained and verified.

2.4.3.6 In the case of a continuing business relationship, the designated institution shall introduce a system of periodical updating of customer identification data.

2.4.3.7 When there is suspicion of money laundering or financing of terrorism, or where there are reasonable grounds to doubt the accuracy or veracity of previously obtained information, the designated institution shall apply enhanced CDD 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.

Additional Identification Requirements for Politically Exposed Persons (PEPs)

2.4.3.8 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 or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc, including their spouses, close relatives and associates or legal persons and arrangements controlled by such persons.

2.4.3.9 A designated institution shall gather sufficient information on any prospective customer falling under this category including checking all the information available on the person in the public domain.

2.4.3.10 The designated institution shall verify the identity of the person and seek information about the source/s of wealth and source/s of funds before accepting the PEP as a customer.

2.4.3.11 The decision to undertake a transaction with a PEP shall be taken at a senior level within the designated institution, and the guidelines for making such decisions shall be clearly spelt out in writing in the customer acceptance policy. The designated institution shall also subject transactions involving a PEP to enhanced monitoring on an ongoing basis.

2.4.3.12 The enhanced due diligence requirements may also be applied to customers who become PEPs subsequent to establishment of the business relationship.

2.4.3.13 These instructions are also applicable to transactions where a PEP is the ultimate beneficial owner.

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

Special Identification Requirements Applicable to MTAs

2.4.3.15 For all remittances received, a MTA should ensure that the complete originator's information is provided. Where, the originator's information is incomplete or unavailable, the MTA is required to adopt an effective risk based approach in deciding whether to proceed, stop or request for the missing originator's information from the corresponding institutions.

2.4.3.16 Remittances with incomplete originator's information may be considered as a factor for suspicion and where appropriate, the MTA should lodge a STR with the Unit.

2.4.3.17 The MTA should have a written policy clearly spelling out the customer identification procedures in the following circumstances:

- when making payment to a beneficiary or

- when the MTA has doubts regarding the authenticity/veracity or the adequacy of previously obtained customer identification data.

2.4.4 **Monitoring of Transactions**

2.4.4.1 Generally, designated institutions transact with occasional, once-off or walk-in customers, and do not normally open or maintain accounts.

2.4.4.2 Where, however, a designated institution has repeat customers or ongoing business relationships, ongoing monitoring becomes essential. Every designated institution is therefore expected to have an understanding of the normal transacting patterns and source of funds of its customers. This will give the designated institution the means to identify transactions that fall outside the regular pattern of activity and, accordingly to file STRs.

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

2.4.4.4 Every designated institution may set limits for any category of transactions and pay particular attention to the receipts which exceed these limits. High-risk receipts have to be subjected to intense monitoring.

2.4.4.5 A designated institution shall set key indicators for such receipts, taking note of the background of the customer e.g. the country of origin, sources of funds, the type of transactions involved and other risk factors.

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

2.4.4.7 Designated institutions shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from countries classified by the FATF as uncooperative or high risk countries that do not sufficiently apply the FATF Standards.

2.4.4.8 Further, 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 should be retained and made available to the Unit and other competent authorities, on request.

2.4.4.9 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. Under these circumstances, the designated institution shall file an STR with the Unit even if the transaction did not go through.

2.5 Risk Management

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

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

2.5.3 Higher risk customers, products and services, including delivery channels, and geographical locations should be identified and commensurate AML / CFT measures applied.

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

- The nature, scale and complexity of the designated institution's operations, including geographical diversity.
- The initial and ongoing due diligence or monitoring conducted on the designated institution's agent locations.
- The designated institution's customer, product, and activity profile.
- The nature of the business relationship (*i.e.* occasional vs. ongoing relationship).
- The distribution channels used.

- The volume and size of transactions.
- 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.

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

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

Controls for Higher Risk Situations

2.5.7 A Designated institution is required to implement appropriate measures and controls to mitigate the potential money laundering or financing of terrorism risks for situations that are considered to be of higher risk as determined from the designated institution's risk assessment.

2.5.8 These measures and controls may include:

- Increased levels of know your customer (KYC) or enhanced due diligence, such as proactive contact with the customer to determine the reason for the transactions, the customer's relationship to the sender or receiver, and the source of funds.
- Increased levels of controls and frequency of reviews of customer relationships.
- Increased transaction monitoring of higher-risk products, services and channels.
- Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent location.
- Aggregation of activity by a known or a new customer.

2.5.9 Designated institutions should pay special attention to any money laundering threats that may arise from new or developing technologies, including internet-based transactions which might favour anonymity; and take measures to prevent their use for money laundering or financing of terrorism.

Implementation of Risk-Based Approach to AML/CFT Programmes

2.5.10 The Unit recognizes the diversity of the institutions it regulates; and it seeks to establish that overall AML/CFT processes appropriate to institutions are in place and are operating effectively.

2.5.11 Designated institutions should formulate and implement a risk-based approach in their AML/CFT programmes.

2.5.12 This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme.

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

2.5.14 While 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.

2.5.15 The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions shall be documented.

2.5.16 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.

2.5.17 A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which

level of management is able to approve business relationships with such customers.

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

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

- Differentiation of client relationships by risk categories (such as high, moderate or low);
- Differentiation of client relationships by risk factors (such as products, client 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 client activity profile).
- KYC documentation and due diligence information requirements appropriate for each risk category and risk factor; and
- Requirements for the approval of upgrading and downgrading of customer risk ratings.

2.5.20 A designated institution shall establish a customer's profile taking into account, at a minimum:

- The nature of the customer's business (whether cash intensive etc);
- The nature and frequency of the activity;
- The complexity, volume and pattern of transactions;
- 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);
- Delivery channels (e.g. whether mobile/internet banking, wire transfers to third parties, remote cash withdrawals);

- Geographical origin of the customer;
- 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);
- Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;
- Unwillingness of the customer to cooperate with the designated institution's customer due diligence process for no apparent reason;
- Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

2.5.21 Accordingly, a designated institution 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. Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is available.

2.5.22 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.

2.5.23 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 to assist in risk categorization.

2.5.24 A designated institution 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.

2.5.25 In addition, a designated institution shall periodically review its risk categories as typologies evolve on practices by money launderers and terrorists. These reviews shall not be undertaken at intervals not longer than one two years.

3 INTERNAL CONTROLS, POLICIES & PROCEDURES

3.1 General

3.1.1 The Board of Directors of a designated institution shall ensure that effective AML/CFT internal controls are put in place by establishing appropriate procedures and ensuring effective implementation.

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

3.1.3 Designated institutions shall devise procedures for creating risk profiles of their existing and new customers and apply various anti money laundering measures, keeping in view the risks involved in a transaction.

3.1.4 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.

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

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

3.2 Appointment Of A Money Laundering Reporting Officer (MLRO)

3.2.1 A designated institution 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;

- Monitoring and reporting of all suspicious transactions and sharing of information as required under the BUP&SML Act,
- Overseeing and ensuring overall compliance with regulatory guidelines on AML/ CFT issues from time to time,
- Developing appropriate compliance management arrangements across the full range of AML/CFT areas (e.g. CDD, record keeping, etc.).
- Maintaining close liaison with law enforcement agencies, other designated institutions and any other institutions that are involved in the fight against money laundering and 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.

3.3 **Recommended Procedures**

3.3.1 Every designated institution shall:

a) Have procedures for the prompt validation of suspicious transactions 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 transaction reports that 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 Section 26 of the BUPSML Act imposes obligations on designated institutions to report suspicious transactions to the Unit.

4.2 A designated institution shall write and submit to the Unit a suspicious transaction report if it has reasonable ground of believing that the transaction, including an attempted transaction, involves proceeds of crime, irrespective of the amount involved.

4.3 The STR shall be furnished to the Unit as soon as reasonably possible but no more than 3 days from date of detection of the suspicious transaction.

4.4 The MLRO shall record his reasons for treating any transaction or a series of transactions as suspicious. The designated institution shall ensure that there is no undue delay in making a decision whether a transaction should be reported as suspicious.

4.5 It is likely that in some cases, transactions are abandoned/ aborted by customers on being asked to give some more details or to provide documents. In such cases, a designated institution shall report every such attempted transaction as an STR, even if the transaction was not completed by the customer, and irrespective of the amount involved.

4.6 In reporting of STRs, a designated institution shall use the STR template provided as **Annexure 1**.

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

Examples of Transactions That May Trigger Suspicion

- Customer is evasive or unwilling to provide information when requested.
- Transactions conducted are out of character with the usual conduct or profile of customers carrying out such transactions.
- Customer using different identifications each time conducting a transaction.
- A group of customers trying to break up a large cash transaction into multiple small transactions.

- The same customer conducting a few small transactions in a day or at different branches/locations.
- There are sudden or inconsistent changes in remittance/wire transfer sent/received transactions.
- Remittances/wire transfers from different customers/jurisdiction being sent to the same customer.
- Customer frequently remitting money to or receiving money from FATF listed non-cooperative countries/jurisdictions.
- Customer exchanging small denomination notes into large denomination notes, in large quantity.
- The same customer frequently exchanging local currency into foreign currency without apparent economic or visible lawful purpose.
- Customer frequently exchanging large amount of foreign currency but not exceeding a laid down limit.
- Customer exchanging cash for numerous postal money orders in small amounts for numerous other parties

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

4.8 Designated institutions shall not put any restrictions on payment to beneficiaries where an STR has been made. Moreover, a designated institution shall ensure that employees keep the fact of furnishing such information as strictly confidential, and **tipping off** to the customer is strictly prohibited.

5 MAINTENANCE OF RECORDS OF TRANSACTIONS

5.1 Section 25 of the BUPSML Act imposes obligations on designated institutions regarding the recording and maintenance of customer information and transactions.

5.2 A designated institution shall take all necessary steps to ensure compliance with the requirements of the Act. The designated institution shall introduce a system of maintaining proper records 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 transaction information to be recorded and maintained include the following:

- Identity of the customer;
- the nature of the transaction;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

5.5 Every designated institution shall take appropriate steps to implement a system that allows data to be retrieved easily and quickly whenever required or when requested by the Unit or by other 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 client.

5.7 In addition to information which all designated institutions are required to record and maintain, a Bureau de Change shall record in the receipt, at a minimum, the following information:

- licensed Bureau de Change's name, business address and telephone number;
- date of transaction;
- receipt serial number;
- amount and type of currency exchanged by the customer;
- amount and type of currency the customer exchanged for;
- exchange rate offered; and

- name and national registration identification card/passport number of the customer.

6 CUSTOMER EDUCATION/EMPLOYEE TRAINING

6.1 Customer Education

6.1.1 Implementation of KYC procedures requires designated institutions to demand certain information from a customer which may be of a 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 and necessity of the KYC policies.

6.1.3 The front desk staff need to be specially trained to handle such situations while dealing with customers.

6.2 Employees' Training

6.2.1 Every designated institution shall conduct an ongoing employee training programme which ensures that members of staff are adequately trained so that they are aware of:

- policies and procedures relating to the prevention and detection of money laundering and counter terrorist financing, and
- the need to monitor all transactions so as to detect and report suspicious activity.

6.2.2 It is important that all staff members fully understand the rationale behind the AML/CFT policies, and the need for them to implement such policies consistently.

6.2.3 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 designated institution, and the respective procedures laid down in writing.

Issued by the Bank Use Promotion and Suppression of Money Laundering Unit, June 2012