United Republic of Tanzania

Financial Intelligence Unit

Anti-Money Laundering Guidelines to Collective Investment Schemes

GUIDELINES NO: 6

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AML	Anti Money Laundering
AMLA	Anti Money Laundering Act, Cap 423, 2006
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CIS	Collective Investment Scheme
CMSA	Capital Markets and Securities Authority
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IOSCO	International Organization of Securities Commissions
LDMS	Licensed Dealing Members
ML	Money Laundering
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
TZS	Tanzanian Shillings
UN	United Nations
UNSCR	United Nations Security Council Resolution

1.0 INTRODUCTION

1.1 The Anti-Money Laundering Act, Cap 423, 2006 (AMLA) was promulgated to make better provisions for the prevention and prohibition of money laundering, to provide for the disclosure of information on money laundering, to establish a Financial Intelligence Unit and the National Multi-Disciplinary Committee on Anti-Money Laundering and to provide for matters connected thereto.

1.2 These guidelines are issued pursuant to Section 6(f) of AMLA and Regulation 32 of the Anti-Money Laundering Regulations, 2007. The guidelines apply to all Collective Investment Schemes in the Tanzanian securities industry.

1.3 A Trustee of a CIS shall ensure that managers of a scheme in which the Trustee is a participating party shall fully comply with these guidelines.

1.4 The ability to launder the proceeds of crime through the financial system is vital for the success of criminals. Those involved need to exploit the facilities of the world's financial institutions if they are to benefit from the proceeds of their illegal activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, goods and services have enhanced the ease with which proceeds of crime can be laundered and have complicated the tracing and tracking process.

1.5 The FATF, an inter-governmental organization which sets international standards to combat money laundering and terrorist financing, noted that some of the features that have long characterized the securities industry, including its speed in executing transactions, its global reach, and its adaptability, can make it attractive to those who would abuse it for illicit purposes, including money laundering and terrorist financing. The FATF also noted that unlike other sectors, the risks lie mainly not in respect of the placement stage of money laundering, but rather in the layering and integration stages. Typical securities-related laundering schemes often involve a series of transactions that do not match the investor's profile and do not appear designed to provide a return on

investment. Suspicious Indicators for Money Laundering and Terrorist Financing in the Securities Industry as compiled by the FATF are given at Appendix A. A list of specific indicators for insider trading, market manipulation and securities fraud are included at Appendix A.

1.6 Market players in the securities sector can be involved, knowingly or unknowingly, in money laundering and the financing of terrorism. This exposes them to legal, operational and reputational risks. The securities sector should therefore take adequate measures to prevent its misuse by money launderers and terrorists.

2.0 CUSTOMER DUE DILIGENCE (CDD)

2.1 Anonymous Account of Fictitious Persons

No CIS manager shall deal with any person on an anonymous basis or any person using a fictitious name.

2.2 CDD Performance

A CIS manager shall perform CDD measures when –

(a) unit holders subscribe or take part in the CIS

(b) the CIS manager enters into negotiations with a entity with a view to signing a trust deed for establishment of a CIS ;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the CIS manager would otherwise not be required by these Guidelines to perform CDD measures, or

(d) the CIS manager has any doubt about the veracity or adequacy of information being provided.

Identification of Customers

2.3 A CIS manager shall establish the identity of each customer who signs an agreement to acquire or repurchase units/shares of a scheme.

2.4 For the purpose of the preceding paragraph, a CIS manager shall obtain and record information of the customer, including but not limited to the following:

(a) In case of natural persons; Full name, age, physical address, occupation, residence, and other particulars that will enable the identification of the individual;

(b) In case of legal persons:

i. Incorporation status, or in a case of a branch of a foreign company, place of incorporation or registration (as may be appropriate)

ii. the incorporation number or business registration number

iii. registered or business address and contact telephone number(s)

iv. Names and particulars of shareholders, if the immediate shareholder is a holding company to determine the ultimate or beneficial shareholders, and

v. Names, addresses and nationalities of directors.

Verification of Identity

2.5 The CIS manager shall verify the identity of a customer using reliable, independent sources.

2.6 The CIS manager shall retain copies of all reference documents used in identity verification and the identification information.

Identification of Beneficial Owners and Verification of their Identity

2.7 The CIS manager shall inquire if there exists any beneficial owner in relation to a customer. "Beneficial owner", in relation to a customer of a CIS manager, means the natural person who makes final decisions, ultimately controls a customer or the person on whose behalf a transaction is being conducted. This includes the person who exercises ultimate effective control over a body corporate or unincorporate.

2.8 Where there is one or more beneficial owners in relation to a customer, the CIS manager shall take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner(s).

2.9 Where the customer is not a natural person, the CIS manager shall take reasonable measures to understand the ownership and structure of the customer.

2.10 The CIS manager shall not be required to inquire if there exists any beneficial owner in relation to a customer that is –

(a) a Tanzanian government entity

(b) a foreign government entity, provided it is not sanctioned or blacklisted by the international community such as the United Nations or FATF

(c) an entity listed on the stock exchange in Tanzania

(d) an entity listed on a stock exchange outside of Tanzania that is subject to adequate regulatory disclosure requirements

(e) a financial institution supervised by the Bank of Tanzania, CMSA or Tanzania Insurance Regulatory Authority

(f) a financial institution incorporated or established outside Tanzania that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF

(g) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme

unless the CMSA licensee suspects that the transaction is connected with money laundering or terrorist financing.

For the purposes of items (d) and (f) above, a CIS manager shall document the basis for its determination that the requirements in those paragraphs have been duly met.

Identification and Verification of Identity of Natural Persons Appointed to Act on Customer's Behalf

2.11 Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the CIS manager or the customer is not a natural person, the CIS manager shall-

(a) identify the natural persons that act or are appointed to act on behalf of the customer, as if such persons were themselves customers

(b) verify the identity of these persons using reliable, independent sources, and

(c) retain copies of all reference documents used to verify the identity of these persons.

2.12 In the case of private trusts, the CIS manager shall verify the authorization given to each trustee of the relevant trust.

2.13 The CIS manager shall verify the due authority of such person to act on behalf of the customer, by obtaining, including but not limited to, the following:

(a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

2.14 Where the customer is a Tanzanian government entity, the CIS manager shall only be required to obtain such information as may be required to confirm that the customer is a Tanzanian government entity as indicated.

Reliance on Identification and Verification Already Performed

2.15 Where a CIS Manager ("acquiring Manager") acquires, either in whole or in part, the business of another CIS Manager, the acquiring Manager, shall perform CDD measures on customers acquired with the business at the time of acquisition, except where the acquiring Manager has :

(a) acquired at the same time all corresponding customer records (including information on natural persons appointed to act or are acting on behalf of the customer) and has no doubt or concerns about the veracity or adequacy of the information so acquired, and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring Manager as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof.

The Trustee of the acquired scheme shall ensure that the new manager fully complies with these guidelines.

Information on the Purpose and Intended Nature of Business Relations

2.16 A CIS manager shall obtain, from a customer, when processing an application to establish business relations, information as to the purpose and intended nature of business relations.

2.17 Time for completion of CDD Measures

(a) No CIS manager shall act as manager for a CIS unless the manager has completed CDD measures in relation to that customer.

(b) If the CIS manager is, for any reason, unable to complete CDD measures on a customer, it shall not enter into a business relationship with that customer and shall instead consider if the circumstances are suspicious so as to warrant the filing of an STR.

Face-to-Face Verification

2.18 A CIS manager shall have at least one face-to-face contact with a customer before allowing that customer to hold units/shares in the CIS.

2.19 Where there is no face-to-face contact, the CIS manager shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

3.0 ONGOING MONITORING

3.1 A CIS manager shall observe conduct of the customer especially the customer's transactions to ensure that such transactions are generally consistent with the CIS Manager's knowledge of the customer.

3.2 A CIS manager shall pay special attention to the transactions conducted by a customer that have no apparent or visible economic or lawful purpose.

3.3 A CIS manager shall, to the extent possible, inquire into the background and purpose of the transactions and document their findings with a view to making this information available to the relevant competent authorities, should the need arise.

3.4 A CIS manager shall periodically review the adequacy of customer identification information obtained in respect of customers (in particular, that of the natural persons appointed to act for the customer) and ensure that the information is kept up to date.

4.0 RECORD KEEPING

4.1 Every CIS manager shall prepare, maintain and retain documentation on all its business relations, transactions (these include account files and business correspondences) with its customers such that –

(a) all requirements imposed by AMLA, Regulations and Guidelines are met

(b) any transaction undertaken by the CIS manager can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal/money laundering activity

(c) the relevant competent authorities in Tanzania and the internal and external auditors of the CIS manager are able to review the entity's transactions and assess the level of compliance with the law, regulations and guidelines, and

(d) the CIS manager can make available records on a timely basis to domestic competent authorities upon appropriate authority for information.

4.2 A CIS manager shall, when setting its record retention policies and performing its internal procedures, comply with the following document retention periods:

(a) a period of at least five years as provided for under Regulation 29 of the Anti-Money Laundering Regulations, 2007.

(b) The document retention period above is subject to paragraph 4.3.

4.3 The reporting entity shall retain records pertaining to a matter which is under investigation or which has been the subject of a suspicious transaction report (STR) for such longer period as may be necessary in accordance with any request or order from relevant competent authorities in Tanzania.

5.0 SUSPICIOUS TRANSACTION REPORTING

5.1 A CIS manager shall keep in mind the provisions in Section 17 (a) and (b) of AMLA and Regulation 20 (1) and (2) of the Anti-Money Laundering Regulations 2007 that provide for reporting to competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to the FIU, and

(b) keep records of all transactions referred to the FIU, together with all internal findings and analysis done in relation to them.

5.2 A CIS manager shall submit reports on suspicious transactions (including attempted transactions) to the FIU.

5.3 A CIS manager shall consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report and document the basis for its determination where -

(a) the CIS manager is for any reason unable to complete CDD measures, or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the CIS manager or decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

6.0 INTERNAL POLICIES, COMPLIANCE, AUDIT, TRAINING AND EMPLOYEE/AGENT SCREENING

6.1 A CIS manager shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees and agents.

6.2 The policies, procedures and controls shall include, among other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.

6.3 A CIS manager shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favor anonymity, in formulating its policies, procedures and controls.

6.4 A CIS manager shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer. The CIS manager shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, have timely access to all customer records and other relevant information which they require to discharge their functions.

6.5 A CIS manager shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the CIS trustee's internal policies, procedures and controls, and its compliance with regulatory requirements.

6.6 A CIS manager shall have in place screening procedures to ensure high standards when hiring employees and agents.

6.7 A CIS manager shall take all appropriate steps to ensure that its staff and agents (whether in Tanzania or overseas) are regularly trained on:

(a) AML/CFT laws, regulations and guidelines, and in particular, CDD measures detecting and reporting suspicious transactions

(b) prevailing techniques, methods and trends in money laundering and terrorist financing, and

(c) the CIS manager's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff and agents in combating money laundering and terrorist financing.

7.0 EFFECTIVE DATE

These guidelines shall become effective on 1st February, 2012.

Herman M. Kessy

Commissioner

Financial Intelligence Unit

APPENDIX A: SUSPICIOUS INDICATORS FOR MONEY LAUNDERING AND TERRORIST FINANCING IN THE SECURITIES INDUSTRY

Customer Due Diligence

- The customer provides the securities firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. This indicator may apply to account openings and to interaction subsequent to account opening, such as wire transfers.
- During the account opening process, the customer refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.).
- The customer, whether a person or entity, is reluctant to provide the securities firm with complete information about the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, the entity's officers and directors or business location.
- The customer, whether a person or entity, is located in a jurisdiction that is known as a bank secrecy haven, a tax shelter, or high-risk geographic locations (e.g. narcotics producing jurisdiction).
- The customer is reluctant to meet personnel from the securities firm in person, is very secretive and/or evasive or becomes defensive when asked to provide more information.
- The customer refuses to identify a legitimate source for funds or provides the securities firm with information that is false, misleading, or substantially incorrect.
- The customer engages in frequent transactions with money services businesses.
- The customer's background, whether a person or entity, is questionable or does not meet expectations based on business activities.
- The customer has no discernable reason for using the firm's service or, the firm's disadvantageous location does not discourage the customer (e.g. customer lacks roots to the local community or has come out of his or her way to use the firm).

- The customer refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.
- The customer's address is associated with multiple other accounts that do not appear to be related.
- The customer has a history of changing financial advisors and/or using multiple firms or banks. This indicator is heightened when the customer uses firms located in numerous jurisdictions.
- The customer is known to be experiencing extreme financial difficulties.
- The customer is, or is associated with, a PEP or senior political figure.
- The customer refuses to invest in more appropriate securities when those securities would require a more enhanced CDD/KYC procedure.
- The customer with a significant history with the securities firm abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.
- The customer appears to be acting as a fiduciary for someone else but is reluctant to provide more information regarding for whom he or she may be acting.
- The customer is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons. Sources for this information include news items or Internet searches.
- The customer inquires as to how quickly he or she can liquidate accounts or earnings without explaining why or provides suspicious reasons for doing so.
- The customer opens an account or purchases a product without any regard to loss, commissions or other costs associated with that account or product.
- The customer has commercial or other types of relationships with risky persons or institutions.
- The customer acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.
- The customer exhibits unusual concern with the securities firm's compliance with government reporting requirements and/or the firm's AML/CFT policies.

- The customer is reluctant to provide the securities firm with information needed to file reports or fails to proceed with a transaction once asked for documentation or learns of any recordkeeping requirements.
- The customer is interested in paying higher charges to the securities firm in order to keep some of his or her information secret.
- The customer tries to persuade an employee of the securities firm not to file a required report or not to maintain required records.
- The customer funds deposits, withdraws or purchases financial or monetary instruments below a threshold amount in order to avoid any reporting or recordkeeping requirements imposed by the jurisdiction.
- The customer requests that account openings and closings in his or her name or in the name of family members be done without producing a paper trail.
- Law enforcement has issued subpoenas regarding a customer and/or account at the securities firm.

Fund Transfers and/or Deposits

- Wire transfers are sent to, or originate from, financial secrecy havens, tax shelters or high-risk geographic locations (e.g. jurisdictions known to produce narcotics/psychotropic drugs or to be related to terrorism) without an apparent business reason or connection to a securities transaction.
- Wire transfers or payments to or from unrelated third parties (foreign or domestic) or where the name or account number of the beneficiary or remitter has not been supplied.
- Many small, incoming wire transfers or deposits are made, either by the customer or third parties, using cheques, money orders or cash that are almost immediately withdrawn or wired out in a manner inconsistent with customer's business or history.
- Incoming payments made by third-party cheques or cheques with multiple endorsements.
- Deposit of large amount of small-denomination currency to fund account or exchanges of small notes for bigger notes.

- Wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.
- The securities account is used for payments or outgoing wire transfers with little or no securities activities (e.g. account appears to be used as a depository account or a conduit for transfers).
- The controlling owner or officer of a public company transfers funds into his personal account or into the account of a private company that he or she owns or that is listed as an authorised signatory.
- Quick withdrawal of funds after a very short period in the account.
- Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.
- Transfers/journals between different accounts owned by the customer with no apparent business purpose.
- Customer requests that certain payments be routed through nostro or correspondent accounts held by the financial intermediary or sundry accounts instead of its own account.

Bearer Securities

- The customer requests cashing bearer securities without first depositing them into an account or frequently deposits bearer securities into an account.
- The customer's explanation regarding the method of acquiring the bearer securities does not make sense or changes.
- The customer deposits bearer securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

Unusual Securities Transactions and Account Activity

- 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.
- A customer's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.
- The purchase and sale of non-listed securities with a large price differential within a short period of time. This may be indicative of transferring value from one party to another.
- Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without indentifying who they are for or providing very little information regarding the underlying account holder or beneficiary.
- A company uses cash to pay dividends to investors.
- Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.
- Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.
- A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).
- A customer's transactions have no apparent economic purpose.
- A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
- Transactions that show the customer is acting on behalf of third parties.
- The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
- Transactions involving an unknown counterparty.
- Large sum cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

Activity that is Inconsistent with the Customer's Business Objective or Profile

- The customer's transaction patterns suddenly change in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.
- There are unusual transfers of funds or journaling (i.e. book entries) among accounts without any apparent business purpose or among apparently unrelated accounts.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- The customer's account is not used for its intended purpose (i.e. used as a depository account).
- The customer enters into a financial commitment that appears beyond his or her means.
- The customer begins to use cash extensively.
- The customer engaged in extremely complex transactions where his or her profile would indicate otherwise.
- Customer's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
- The time zone in customer's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the customer's typical business activity.
- A foreign based customer that uses domestic accounts to trade on foreign exchanges.
- The customer exhibits a lack of concern about higher than normal transaction costs.

Rogue Employees

- The employee appears to be enjoying a lavish lifestyle that inconsistent with his or her salary or position.
- The employee is reluctant to take annual leave.
- The employee is subject to intense job-related demands, such as sales or production goals that may make him more willing to engage in or overlook behaviour that poses ML/TF risks.
- The employee inputs a high level of activity into one customer account even though the customer's account is relatively unimportant to the organisation.
- The employee is known to be experiencing a difficult personal situation, financial or other.

- The employee has the authority to arrange and process customer affairs without supervision or involvement of colleagues.
- The management/reporting structure of the financial institution allow an employee to have a large amount of autonomy without direct control over his activities.
- The employee is located in a different country to his direct line of management, and supervision is only carried out remotely.
- A management culture within the financial institution focuses on financial reward over compliance with regulatory requirements.
- The employee's supporting documentation for customers' accounts or orders is incomplete or missing.
- Business is experiencing a period of high staff turnover or is going through significant structural changes.