United Republic of Tanzania

Financial Intelligence Unit

Anti-Money Laundering Guidelines to CMSA Licensees

GUIDELINES NO: 5

TABLE OF CONTENTS

ACRONYMS

AML	Anti Money Laundering
AMLA	Anti Money Laundering Act, Cap. 423, 2006
BoT	Bank of Tanzania
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CIS	Collective Investment Schemes
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
TIRA	Tanzania Insurance Regulatory Authority
TZS	Tanzanian Shillings
UN	United Nations
UNSCR	United Nations Security Council Resolution

1.0 INTRODUCTION

1.1 The Anti-Money Laundering Act, Cap 423 of 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 licensed market players/intermediaries in the Tanzanian securities industry which include Licensed Dealing Members, Investment Advisors, Custodians of Securities, Promoters, Nominated Advisors, Fund Managers and Investment Management companies.

1.3 These guidelines shall not apply to Collective Investment Schemes (CIS) Trustees. CIS Trustees are governed by separate 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 such as banks and securities companies, 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. Moreover, the securities sector is perhaps unique among industries in that it can be used both to launder illicit funds obtained elsewhere, and to generate illicit funds within

the industry itself through fraudulent activities. 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.

1.6 CMSA licensees 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 CMSA licensee shall deal with any person on an anonymous basis or any person using a fictitious name.

2.2 When CDD is to be performed

A CMSA licensee shall perform CDD measures when –

(a) the CMSA licensee establishes business relations with any customer

(b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the CMSA licensee would otherwise not be required by this set of Guidelines to perform CDD measures, or

(c) the CMSA licensee has doubts about the veracity or adequacy of any information previously obtained.

2.3 Identification of Customers, Beneficial Owners and Verification of their Identities

CDD Measures where Business Relations are Established

(I) Identification of Customers

2.3.1 A CMSA licensee shall identify each customer who applies to the CMSA licensee to establish business relations.

2.3.2 For the purpose of paragraph 2.3.1, a CMSA licensee shall obtain and record information of the customer in accordance with AMLA, including but not limited to the following:

(a) Full name, including any aliases

(b) Unique identification number (such as an identity card number, birth certificate number, voter registration card number or passport number,

or where the customer is not a natural person, the incorporation number or business registration number)

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s)

(d) Date of birth, incorporation or registration (as may be appropriate), and

(e) Nationality or place of incorporation or registration (as appropriate).

2.3.3 Where the customer is a company, the CMSA licensee shall, apart from identifying the customer, also identify the directors of the company.

2.3.4 Where the customer is a partnership or a limited liability partnership, the CMSA licensee shall, apart from identifying the customer, also identify the partners.

2.3.5 Where the customer is any other body corporate or unincorporate, the CMSA licensee shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporate.

(II) Verification of Identity

2.3.6 A CMSA licensee shall verify the identity of the customer using reliable, independent sources.

2.3.7 A CMSA licensee shall retain copies of all reference documents used to verify the identity of the customer.

2.4 Identification of Beneficial Owners and Verification of their Identity

2.4.1 A CMSA licensee shall inquire if there exists any beneficial owner in relation to a customer. "Beneficial owner", in relation to a customer of a CMSA licensee, 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.

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

2.4.3 Where the customer is not a natural person, the CMSA licensee shall take reasonable measures to understand the ownership and structure of the customer.

2.4.4 A CMSA licensee 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 BoT, CMSA or TIRA

(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 CMSA licensee shall document the basis for its determination that the requirements in those paragraphs have been duly met.

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

2.5.1 Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the CMSA licensee or the customer is not a natural person, a CMSA licensee 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.

2.5.2 In the case of private trusts, a CMSA licensee shall verify the authorization given to each trustee of the relevant trust.

2.5.3 A CMSA licensee 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.

2.5.4 Where the customer is a Tanzanian government entity, the CMSA licensee shall only be required to obtain such information as may be required to confirm that the customer is a Tanzanian government entity as indicated.

2.6 Reliance on Identification and Verification Already Performed

When a CMSA licensee ("acquiring CMSA licensee") acquires, either in whole or in part, the business of another financial institution (whether in Tanzania or elsewhere), the acquiring CMSA licensee shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring CMSA licensee has:

(a) acquired at the same time all corresponding customer records (including customer identification information) 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 CMSA licensee as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring CMSA licensee.

2.7 Information on the Purpose and Intended Nature of Business Relations

A CMSA licensee shall obtain, from the customer, when processing the application to establish business relations, information as to the purpose and intended nature of business relations.

2.8 Timing for Verification

Subject to paragraph 2.8.2 of this Guideline, a CMSA licensee shall complete verification of the identity of the customer and beneficial owner:

(a) before the CMSA licensee establishes business relations, or

(b) before the CMSA licensee undertakes any transaction for a customer, where the customer does not have business relations with the CMSA licensee.

2.8.1 A CMSA licensee may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner if -

(a) the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations, and

(b) the risks of money laundering and terrorist financing can be effectively managed by the CMSA licensee.

2.8.2 Where the CMSA licensee establishes business relations before verification of the identity of the customer or beneficial owner, it should adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. The CMSA licensee shall complete such verification as soon as is reasonably practicable. In addition, the CMSA licensee should be ready to explain to competent authorities why the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations.

2.9 Where CDD Measures are Not Completed

Where the CMSA licensee is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report (STR).

2.10 Existing Customers

A CMSA licensee shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

2.11 Joint Account

In the case of a joint account, a CMSA licensee shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the CMSA licensee.

2.12 CDD Measures for Non-Account Holders

2.12.1 A CMSA licensee that undertakes any transaction with a non-account holder shall:

(a) establish and verify the identity of the customer as if the customer had applied to the CMSA licensee to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

2.12.2 Where a CMSA licensee suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this set of guidelines, the CMSA licensee shall treat the transactions as a single transaction and aggregate their values for the purpose of this set of guidelines.

3.0 ENHANCED DUE DILIGENCE - POLITICALLY EXPOSED PERSONS

3.1 A CMSA licensee shall, in relation to politically exposed persons (as defined in AMLA), perform enhanced CDD measures in addition to normal CDD measures, including but not limited to the following:

(a) implement appropriate internal policies, procedures and risk management systems to determine if a customer or beneficial owner is a politically exposed person

(b) obtain approval from the CMSA licensee's senior management to establish or continue business relations where the customer or beneficial owner is a politically exposed person or subsequently found to be or subsequently becomes a politically exposed person

(c) take reasonable measures to establish the source of wealth and source of funds of the customer or beneficial owner, and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

4.0 ENHANCED DUE DILIGENCE - OTHER HIGHER RISK CATEGORIES OF CUSTOMERS

4.1 A CMSA licensee shall perform enhanced CDD measures in paragraph 3 for such other categories of customers, business relations or transactions as the CMSA licensee may assess to present a higher risk for money laundering and terrorist financing.

4.2 A CMSA licensee shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the CMSA licensee for itself or notified to CMSA licensees generally by the Tanzania FIU.

5.0 MEASURES TO ADDRESS THE USE OF NEW TECHNOLOGIES AND NON-FACE-TO-FACE BUSINESS VERIFICATION

5.1 A CMSA licensee shall put in place policies and procedures to address any specific risks associated with the use of new technologies and non-face-to-face business relations or transactions.

5.2 A CMSA licensee shall implement the policies and procedures referred to in paragraph 5.1 when establishing customer relationships and when conducting ongoing due diligence.

5.3 Where there is no face-to-face contact, the CMSA licensee 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.

6.0 RELIANCE ON INTERMEDIARIES TO PERFORM CDD MEASURES

6.1 A CMSA licensee may rely on an intermediary to perform CDD measures in accordance with the Law and regulations if the following requirements are met:

(a) the CMSA licensee is satisfied that the intermediary it intends to rely upon is subject to supervision for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements

(b) the intermediary is not one on which CMSA licensees have been specifically precluded by relevant Tanzanian authorities from relying, and

(c) the intermediary is able and willing to provide, without delay, upon the CMSA licensee's request, any document obtained by the intermediary which the CMSA licensee would be required or would want to obtain.

6.2 No CMSA licensee shall rely on an intermediary to conduct ongoing monitoring of customers.

6.3 Where a CMSA licensee relies on an intermediary to perform the CDD measures, it shall:

(a) document the basis for its satisfaction that the requirements in paragraph 6.1a have been met, and

(b) immediately obtain from the intermediary the information relating to CDD measures obtained by the intermediary.

6.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the CMSA licensee shall remain responsible for its AML/CFT obligations as required under the Law, Regulations and guidelines.

7.0 RECORD KEEPING

7.1 Every CMSA licensee 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 CMSA licensee 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 CMSA licensee are able to review the entity's transactions and assess the level of compliance with the law and regulations, and

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

7.2 A CMSA licensee 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 7.3.

7.3 A CMSA licensee 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.

8.0 ONGOING MONITORING AND PAYING ATTENTION TO UNUSUAL TRANSACTIONS

8.1 A CMSA licensee shall monitor on an ongoing basis, its business relations with customers.

8.2 A CMSA licensee shall, during the course of business relations, observe the conduct of the customer's policy and scrutinize transactions undertaken to ensure that the transactions are consistent with the CMSA licensee's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

8.3 A CMSA licensee shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

8.4 A CMSA licensee shall take reasonable steps to inquire into the background and purpose of the transactions in paragraph 8.3 and document such information and its findings. The records shall be kept for at least seven years with a view to making this information available to the relevant competent authorities should the need arise.

9.0 ENSURING CUSTOMER INFORMATION IS KEPT UP-TO-DATE

A CMSA licensee shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

10.0 SUSPICIOUS TRANSACTION REPORTING

10.1 A CMSA licensee 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.

10.2 A CMSA licensee shall submit reports on suspicious transactions (including attempted transactions) to the FIU.

10.3 A CMSA licensee 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 CMSA licensee 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 CMSA licensee, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

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

11.1 A CMSA licensee 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.

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

11.3 In formulating its policies, procedures and controls, a CMSA licensee 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.

11.4 A CMSA licensee shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT officer. The CMSA licensee shall ensure that the AML/CFT 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.

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

11.6 A CMSA licensee shall have in place screening procedures to ensure high standards when hiring employees and agents.

11.7 A CMSA licensee 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 and regulations, 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 CMSA licensee'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.

12.0 **FOREIGN BRANCHES AND SUBSIDIARIES**

12.1 A CMSA licensee that is incorporated in Tanzania shall develop a group policy on AML/CFT and extend this to all its branches and subsidiaries where applicable outside Tanzania.

12.2 Where a CMSA licensee has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the CMSA licensee for

12.3 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Tanzania, the CMSA licensee shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

12.4 Where the law of the host country or jurisdiction conflicts with Tanzania Law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the CMSA licensee's head office shall report this to the FIU/CMSA and comply with such further directions as may be given by the Authority.

13.0 **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.