

The United Republic of Tanzania

Financial Intelligence Unit



Anti-Money Laundering Guidelines to Banking Institutions

GUIDELINES NO: 2

Table of Contents	Page
1.0 INTRODUCTION	1
2.0 POLICIES, PROCEDURES, PROGRAMS AND CONTROLS	2
3.0 KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE, CUSTOMER IDENTITY VERIFICATION AND RECORD KEEPING ...	3
4.0 REPORTING AND ESTABLISHING CONTACT POINT WITH THE FINANCIAL INTELLIGENCE UNIT	6
5.0 APPOINTMENT AND ROLE OF MONEY LAUNDERING REPORTING OFFICER	7
6.0 STAFF TRAINING AND AWARENESS	9
7.0 PROTECTION OF REPORTING PERSONS AND STAFF	11
8.0 TIPPING OFF	11
9.0 REVIEW OF THE GUIDELINES.....	11
10.0 EFFECTIVE DATE.....	11
APPENDIX A.....	12
1. Money Laundering Using Cash Transactions	12
2. Money Laundering Using Institution's Accounts	13
3. Money Laundering Using Investment Related Transactions	14
4. Money Laundering by International Activity	14
5. Money Laundering by Secured and Unsecured Lending	15
6. Money Laundering Involving Financial Institution Employees and Agents.....	15
7. Sales and Dealing Staff	15
8. Potentially Suspicious Circumstances – Trust Companies	17

1.0 INTRODUCTION

- 1.1 The Anti-Money Laundering Act, 2006 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 The Anti-Money Laundering Act, 2006 makes general provision for;
 - a) Establishment of a National Multi-Disciplinary Committee on Anti-Money Laundering,
 - b) Establishment of the Financial Intelligence Unit,
 - c) Predicate offences,
 - d) Offences of money laundering,
 - e) Penalties for acts of money laundering,
 - f) Reporting persons,
 - g) Regulators,
 - h) Reporting persons to verify customer's identity,
 - i) Reporting persons to establish and maintain customer records,
 - j) Reporting persons to report suspicious transactions,
 - k) Reporting persons to establish and maintain internal reporting procedures,
 - l) Other preventive measures by reporting persons,
 - m) Tipping off,
 - n) Override of secrecy obligation,
 - o) Protection of reporting persons,
 - p) Obligation to report physical cross boarder transportation of cash or bearer negotiable instruments.
- 1.3 These guidelines are issued pursuant to Section 6 (f) of the Anti-Money Laundering Act, 2006 and Regulation 32 (1) (c) of the Anti-Money Laundering Regulations, 2007.
- 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 banking 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 most common form of money laundering that banking institutions will encounter on a day to day basis, in respect of their mainstream banking business, takes the form of accumulated cash transactions which will be deposited in the

banking system or exchanged for value. Electronic funds transfer systems increase vulnerability by enabling cash deposits to be switched rapidly between accounts in different names and different jurisdictions. Banking institutions, as providers of a wide range of services are vulnerable to being used in the layering and integration stages. Mortgage and other loan accounts may be used as part of this process to create complex layers of transactions.

- 1.6 Banking institutions have an indispensable role to play in combating money laundering and terrorism financing given their unique position and role in the financial system and economy.

2.0 POLICIES, PROCEDURES, PROGRAMS AND CONTROLS

- 2.1 Banking institutions should put in place policies, programs and procedures for detecting and preventing Money Laundering and Financing of Terrorism. The policies should provide for monitoring and control of Money Laundering and Financing of Terrorism risks at the highest level.
- 2.2 All banking institutions should ensure from time to time compliance with policies, procedures, programs and controls for combating money laundering and financing of terrorism to satisfy the requirements of the law.
- 2.3 Banking institutions are required to establish clear responsibilities and accountabilities to ensure that policies, procedures, programs and controls which deter criminals from using their facilities for money laundering, are implemented and maintained, thus ensuring that they comply with the law.
- 2.4 The policies must provide for, among other things:
 - a) Training of staff on AML/CFT issues.
 - b) Customer identification in line with the law and implementing regulations.
 - c) Record keeping in accordance with the law and implementing regulations.
 - d) Know Your Customer and Customer Due Diligence,
 - e) Enhanced Due Diligence in the case of large, complex or unusual transactions and transactions with Politically Exposed Persons.
 - f) The appointment of an AML/CFT Reporting Officer at Senior Management level.
- 2.5 Banking institutions should develop programs against money laundering and terrorism financing. These programs should include:

- a) Development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
- b) Ongoing employee-training program.
- c) Audit function to test the consistency and robustness of the system.

3.0 KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE, CUSTOMER IDENTITY VERIFICATION AND RECORD KEEPING

- 3.1 Banking institutions must have sound Know Your Customer (KYC) policies and procedures, which are a critical element in anti-money laundering and the effective management of banking risks. Sound KYC procedures help to protect banking institutions' reputation and the integrity of banking systems by reducing the likelihood of banking institutions to be vehicles for or victims of financial crime, reputation damage and financial losses.
- 3.2 Key elements in the design of KYC programs should include customer acceptance policy, customer identification, on going monitoring of high-risk accounts and risk management.
- 3.3 Banking institutions should not keep anonymous accounts or accounts in fictitious names. They should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:
 - a) Establishing business relations;
 - b) Carrying out occasional transactions;
 - c) There is a suspicion of money laundering or terrorism financing;
 - d) There are doubts about the veracity or adequacy of previously obtained customer identification information.
- 3.4 Banking institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks and should also guard against establishing relations with respondent foreign banking institutions that permit their accounts to be used by shell banks.
- 3.5 Banking institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, banking institutions should have policies and procedures in place to address any specific risks associated with non face-to-face business relationships or transactions.

- 3.6 Banking institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or viable lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established, put in writing, and made available to help competent authorities.
- 3.7 The customer due diligence (CDD) measures to be taken includes the following;
- a) Identifying the customer and verifying customer's identity using reliable, independent source documents, data or information.
 - b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the banking institution is satisfied that it knows who the beneficial owner is.
 - c) Obtaining information on the purpose and intended nature of the business relationship.
 - d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including the source of funds.
- 3.8 Banking institutions should apply each of the CDD measures pointed out above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, institutions should perform enhanced due diligence.
- 3.9 Banking institutions, like all reporting persons, must verify identities of the customers they deal with in line with the provisions of the Act, implementing regulations and guidelines.
Banking institutions should verify the identities of customers and beneficial owners before or during the course of establishing a business relationship or conducting transactions for walk in customers. Where the institution is unable to verify the identity as above, it should not open the account, commence business relations or conclude the transaction; or should terminate the business relationship; and file a suspicious activity report in relation to the customer. Institutions should conduct due diligence on such existing relationships at appropriate times.

3.10 Banking institutions should, in relation to politically exposed persons (as defined in the Act), in addition to performing normal due diligence measures:

- a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
- b) Obtain senior management approval for establishing business relationships with such customers.
- c) Take reasonable measures to establish the source of wealth and source of funds.
- d) Conduct enhanced ongoing monitoring of the business relationship.

3.11 In relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures, banking institutions need to:

- a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorism financing investigation or regulatory action;
- b) Assess the respondent institution's anti-money laundering and terrorism financing controls;
- c) Obtain approval from senior management before establishing new correspondent relationships;
- d) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

3.12 Banking institutions must retain records concerning customer identification and transaction. This is an essential constituent of the audit trail. If the Financial Intelligence Unit and law enforcement agencies investigating a money laundering case cannot link criminal funds passing through the financial system with the original criminal proceeds generating such funds, then confiscation of the criminal proceeds cannot be effected. The most important role a banking institution can play in a money laundering investigation is through the provision of relevant records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail.

- 3.13 The records prepared and maintained by any banking institution on its customer relationships and transactions should ensure that:
- a) Requirements of legislation are fully met;
 - b) Competent third parties will be able to assess the institution's observance of anti-money laundering and anti-terrorism financing policies and procedures;
 - c) Any transactions effected via the institution can be reconstructed; and,
 - d) The institution can satisfy enquiries from the appropriate authorities.
- 3.14 Banking institutions are required to retain records for at least five years as provided for under regulation 29 of the Anti-Money Laundering Regulations 2007. Retention may be by way of original documents, stored on hard copy files, microfiche, and computer disk or in other electronic form.
- 3.15 Banking institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions including the amounts and types of currency involved so as to provide, if necessary, evidence for prosecution of criminal activity.
- 3.16 Banking institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended. The identification data and transaction records should be available to domestic competent authorities upon appropriate authority's request.

4.0 REPORTING AND ESTABLISHING CONTACT POINT WITH THE FINANCIAL INTELLIGENCE UNIT

- 4.1 Banking institutions and FIU need to establish contact points for handling AML/CFT issues including reported suspicious transactions/activities.
- 4.2 Banking institutions must have internal reporting mechanisms on unusual suspicious activities and transactions.
- 4.3 If a banking institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorism financing, it should report promptly its suspicions to the Financial Intelligence Unit as provided for under Section 17 of the Act.

- 4.4 Banking institutions are required to report suspicious transactions to the Financial Intelligence Unit. Generally suspicious transactions will be inconsistent with a customer's known, legitimate business or personal activities for the type of account. The first step to recognition of a suspicious transaction is to know enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.
- 4.5 Efforts to recognize suspicious circumstances should start with the request to open an account or execute the initial transaction.
- 4.6 Examples of what might constitute suspicious transactions are given in Appendix A. Examples given are not intended to be exhaustive and only provide examples of the most basic ways by which money may be laundered. The Financial Intelligence Unit realizes that new typologies of money laundering are constantly evolving.
- 4.7 The national focal point for receiving suspicious transaction/activity reports is the Financial Intelligence Unit.
- 4.8 The use of a standard format issued by the FIU in the reporting of disclosures is important and should be followed. Suspicious transaction reports can be forwarded to the Financial Intelligence Unit in writing, by post, facsimile message or electronic mail, and in cases of urgency; reports may be made orally and followed up with formal written reports. Sufficient information should be disclosed to indicate the nature of transaction/activity and reason for the suspicion.
- 4.9 Following the submission of a suspicious transaction report, any institution is not precluded from subsequently terminating its relationship with the customer provided it does so for commercial or risk containment reasons and does not alert the customer to the fact of the disclosure which would constitute tipping off.

5.0 APPOINTMENT AND ROLE OF MONEY LAUNDERING REPORTING OFFICER

- 5.1 Banking institutions are required to appoint a "Money Laundering Reporting Officer" (MLRO) to whose responsibility will include ensuring that suspicious transactions reports are filed with the FIU. The Money Laundering Reporting Officer should be known to the FIU.
- 5.2 Banking institutions should provide the Money Laundering Reporting Officer with the necessary access to systems and records to discharge his or her duties efficiently and effectively.

- 5.3 Banking institutions' employees should report suspicions of money laundering or terrorism financing to the MLRO.
- 5.4 All banking institutions have an obligation to ensure:
- a) That each employee knows to which person he or she should report suspicions;
 - b) That there is a clear reporting chain under which those suspicions will be passed without delay to the Money Laundering Reporting Officer; and
 - c) That the Money Laundering Reporting Officer should have full access to information in order to facilitate the expeditious reporting of all suspicious transactions to the Financial Intelligence Unit.
- 5.5 The level of a person appointed as Money Laundering Reporting Officer will depend upon the size of the banking institution and the nature of its business, but he or she should be sufficiently senior to command the necessary authority.
- 5.6 The Money Laundering Reporting Officer is required to determine whether the information or other matters contained in the transaction report he or she has received gives rise to knowledge or suspicion that a customer is engaged in money laundering or financing of terrorism.
- 5.7 In making the judgment, on the report received pursuant to para 5.6, the Money Laundering Reporting Officer should consider all other relevant information available within the institution concerning the person or business to whom the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and reference to identification records held. If, after completing this review, he or she decides that the initial report gives rise to knowledge or suspicion of money laundering or terrorism financing, then he or she must report this information to the Financial Intelligence Unit.
- 5.8 The "determination" by the Money Laundering Reporting Officer implies a process with at least some formality attached to it, however minimal. It does not necessarily imply that he or she must give his or her reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for his or her own protection, for internal procedures to require that only written reports are submitted to him or her and that he or she should record his or her determination in writing, and the underlying reasons thereof. The Money Laundering Reporting Officer will be expected to act honestly and reasonably and make his or her determination in good faith.

6.0 STAFF TRAINING AND AWARENESS

- 6.1 Banking institutions must take appropriate measures to make employees aware of:
- a) Policies and procedures put in place to detect, prevent and deter money laundering including those for customer identification, record keeping and internal reporting;
 - b) The relevant legislation pertaining to anti- money laundering, and provide employees with training in the recognition and handling of suspicious transactions.
- 6.2 The effectiveness of the procedures and recommendations contained in these guidelines depend on the extent to which staff in banking institutions appreciate the serious nature of the background against which these guidelines have been issued. As such staff must understand clearly effects of money laundering and terrorism financing and the need to fight money laundering and combat terrorism financing.
- 6.3 It is important that banking institutions should introduce comprehensive measures to ensure that staff are fully aware of their responsibilities. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with the law, regulations, guidelines and internal procedures.
- 6.4 Staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions without fear of reprisal.
- 6.5 Timing and content of training for various categories of staff will need to be adapted by individual institutions for their own needs; however, at least once a year, banking institutions should provide employees with appropriate training in the recognition and handling of transactions carried out by persons who may be engaged in money laundering or terrorism financing. The following is recommended:

(a) New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting of any suspicious transactions to the Money Laundering Reporting Officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority, within the first month of their employment. They should be made aware of the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect.

They should also be provided with a copy of the written policies and procedures in place in the institution for the reporting of suspicious transactions. They should also be made aware of legislation and international standard setters like the United Nations and Financial Action Task Force.

(b) Cashiers/Foreign Exchange Operators/Advisory Staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the institutions' reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

All front line staff should be made aware of the business policy and procedures for dealing with occasional customers, particularly where large cash transactions, money transfers, negotiable instruments, certificates of deposit or letters of credit and other guarantees, are involved, and of the need for extra vigilance in these cases.

Branch staff should be trained to understand that criminal money is not only paid in or drawn out across branch counters and should be encouraged to take note of credit and debit transactions from other sources, e.g., credit transfers, wire transfers and ATM transactions.

(c) Account/Facility Opening Personnel

Staff responsible for account/facility opening and acceptance of new customers must receive the basic training given to cashiers or tellers. In addition, further training should be provided in respect of the need to verify a customer's identity and customer/client verification procedures. They should also be familiarised with the business' suspicious transaction reporting procedures.

(d) Administration/Operations, Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from non-reporting and for assisting money launderers; internal reporting procedures; and, the requirements for verification of identity, the retention of records, and disclosure of suspicious transaction reports under the Anti-Money Laundering Act, 2006, implementing regulations and guidelines from the FIU.

(e) Money Laundering Reporting Officer

In-depth training concerning all aspects of the legislation and internal policies will be required for the Money Laundering Reporting Officer. In addition, the Money Laundering Reporting Officer will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious transactions, the feedback arrangements, new trends and patterns of criminal activity.

(f) Refresher training to all staff

It will also be necessary to make arrangements for refresher training at least annually to ensure that staff do not forget their responsibilities and keep abreast of new developments on AML/CFT.

7.0 PROTECTION OF REPORTING PERSONS AND STAFF

Banking institutions, their directors, officers and employees should be made aware that they are protected by Section 22 (1) of the Anti-Money Laundering Act, 2006 from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether the illegal activity actually occurred.

8.0 TIPPING OFF

Banking institutions, their directors, officers and employees are prohibited by section 20 of the Anti-Money Laundering Act, 2006 from disclosing to the customer the fact that a suspicious transaction report or related information is being reported to the FIU.

9.0 REVIEW OF THE GUIDELINES

Banking institutions are encouraged to compile and record any comments, which arise relative to these Guidelines, and forward them to the Financial Intelligence Unit for its appropriate action.

10.0 EFFECTIVE DATE

These Guidelines become effective on 1st April, 2009


Herman M. Kessy
Commissioner
Financial Intelligence Unit

APPENDIX A

EXAMPLES OF SUSPICIOUS TRANSACTIONS

1. Money Laundering Using Cash Transactions

- (a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- (b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- (c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
- (d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g., cheques, Letters of Credit, Bills of Exchange, etc.)
- (e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.
- (f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
- (g) Frequent exchange of cash into other currencies without exchange control approval.
- (h) Customers whose deposits contain counterfeit notes or forged instruments.
- (i) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- (j) Large cash deposits using night safe facilities, thereby avoiding direct contact with institution staff.

2. Money Laundering Using Institution's Accounts

- (a) Customers who wish to maintain a number of trustee or customers accounts which do not appear consistent with the type of business, including transactions, which involve nominee names.
- (b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- (c) Any individual or company whose account shows virtually no normal face to face banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his/her business (e.g., a substantial increase in turnover on an account).
- (d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- (e) Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- (f) Matching of payments out with credits paid in by cash on the same or previous day.
- (g) Paying in large third party cheques endorsed in favour of the customer.
- (h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- (i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- (j) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client companies and trust accounts.
- (k) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
- (l) Large number of individuals making payments into the same account without an adequate explanation.

3. Money Laundering Using Investment Related Transactions

- (a) Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.
- (b) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas institutions in known drug trafficking areas.
- (c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.
- (d) Larger or unusual settlements of securities in cash form.
- (e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering by International Activity

- (a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.
- (b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- (c) Customers who make regular and large payments, including wire transfers, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs and proscribed terrorist organizations.
- (d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.
- (e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.
- (f) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments.
- (g) Frequent paying in of travellers cheques or foreign currency drafts, particularly if originating from overseas.

5. Money Laundering by Secured and Unsecured Lending

- (a) Customers who repay problem loans unexpectedly.
- (b) Request to borrow against assets held by the banking institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- (c) Request by a customer for a banking institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

6. Money Laundering Involving Financial Institution Employees and Agents

- (a) Changes in employee characteristics (e.g., lavish lifestyles or avoiding taking holidays).
- (b) Changes in employee or agent performance (e.g., the salesman selling products for cash has a remarkable or unexpected increase in performance).
- (c) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

7. Sales and Dealing Staff

(a) New Business

Although long-standing customers may be laundering money through an investment business, it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies. Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

- (a) A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.
- (b) A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
- (c) A client with no discernible reason for using the firm's service;

e.g., clients with distant addresses who could find the same service nearer their home base, or clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

- (d) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.
- (e) Any transaction in which the counterparty to the transaction is unknown.

(b) Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries. However, this is also a useful tactic, which may be used by the money launderer to delay, obscure or avoid detection. Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

(c) Dealing Patterns and Abnormal Transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

(i) Dealing Patterns

- (a) A large number of security transactions across a number of jurisdictions.
- (b) Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business, which the investor operates.
- (c) Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual;
- (d) A client with no discernible reason for using the firm's service; e.g., clients with distant addresses who could find the same service nearer their home base, or clients whose

requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

- (e) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.
- (f) Any transaction in which the counterparty to the transaction is unknown.

8. Potentially Suspicious Circumstances – Trust Companies

The following are examples of potentially suspicious circumstances, which may give rise to a suspicion of money laundering in the context of Trust Companies:

Suspicious Circumstances Relating to the Customer/Client's Behavior:

- (a) The establishment of companies or trusts, which have no obvious commercial purpose;
- (b) Clients/customers who appear uninterested in legitimate tax avoidance schemes;
- (c) Sales invoice totals exceeding the known value of goods;
- (d) The client/customer makes unusually large cash payments in relation to business activities, which would normally be paid by cheques, bankers drafts, etc;
- (e) The customer/client pays either over the odds or sells at undervaluation;
- (f) Customer/clients have a myriad of bank accounts and pay amounts of cash into all those accounts, which, in total, amount to a large overall sum;
- (g) Customers/clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- (h) The payment into bank accounts of large third party cheques endorsed in favour of the client/customer.

Potentially Suspicious Secrecy may involve the following:

- (a) The excessive or unnecessary use of nominees;
- (b) The unnecessary granting of wide ranging Powers of Attorney;
- (c) The utilization of a client account rather than the payment of things directly;

- (d) The performance of "execution only" transactions;
- (e) An unwillingness to disclose the sources of funds;
- (f) The use of a mailing address for non-residents;
- (g) The tardiness and/or unwillingness to disclose the identity of the ultimate beneficial owners or beneficiaries.

Suspicious Circumstances in Groups of Companies and/or Trusts:

- (a) Companies, which continually make substantial losses;
- (b) Complex group structures without a cause;
- (c) Subsidiaries, which have no apparent purpose;
- (d) A frequent turnover in shareholders, directors or trustees;
- (e) Uneconomic group structures for tax purposes;
- (f) The use of bank accounts in several currencies for no apparent reason;
- (g) The existence of unexplained transfers of large sums of money through several bank accounts.

NOTE: It should be noted that none of these factors on their own necessarily mean that a customer/client or any third party is involved in any money laundering. However, in most circumstances a combination of some of the above factors should arouse suspicion. In any event, what does or does not give rise to a suspicion will depend on the particular circumstances.