GUIDELINES ON PREVENTION OF MONEY LAUNDERING & TERRORISM FINANCING FOR CAPITAL MARKET INTERMEDIARIES

Date Issued: 31 March 2004
Revised Edition: 11 January 2007

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR CAPITAL MARKET INTERMEDIARIES

1. PURPOSE

1.1 The Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries are issued pursuant to section 158 of the Securities Commission Act 1993. A failure to comply with any of the requirements of this Guideline by a reporting institution or its representatives (where applicable), will in the absence of extenuating circumstances, reflect adversely on their fitness and properness.

1.2 These Guidelines seek to provide guidance to reporting institutions such as Dealers, Fund Managers, Futures Brokers and Futures Fund Managers licensed under the Securities Industry Act 1983 ("SIA") and Futures Industry Act 1993 ("FIA") and management companies approved by the Securities Commission under the Securities Commission Act 1993 ("SCA") for compliance with the provisions of the Anti-Money Laundering Act 2001 ("AMLA").

2. DEFINITIONS

In these Guidelines, unless the context otherwise requires:

2.1 **"FIU"** means the Financial Intelligence Unit in Bank Negara Malaysia, which is the competent authority as established under subsection 7(1) of the AMLA;

"management company" has the same meaning as is assigned to that expression in the SCA;

"money laundering" means the act of a person who-

(a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity;

(b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Malaysia proceeds of any unlawful activity; or

(c) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity.

"reporting institution" means licensed dealers, fund managers, futures brokers and futures fund managers as licensed under the Securities Industry Act 1983 and Futures Industry Act 1993 and any management company approved under the Securities Commission Act 1993;

"SC" means the Securities Commission;

"serious offence" means:

(a) any of the offences specified in the Second Schedule of the AMLA such as drug trafficking, arms smuggling, insider trading, etc.;

(b) an attempt to commit any of those offence; or

(c) the abetment of any of those offences;

"unlawful activity" means any activity which is related, directly or indirectly, to any serious offence;

3. GENERAL DESCRIPTION OF MONEY LAUNDERING

3.1 In principle, money laundering is a process intended to conceal the benefits derived from unlawful activities which are related, directly or indirectly, to any serious offence so that they appear to have originated from a legitimate source.

3.2 Under the AMLA, any person who:

(a) engages in, or attempts to engage in; or

(b) abets the commission of,

money laundering, commits an offence and shall on conviction be liable to a fine not exceeding five million ringgit or to imprisonment for a term not exceeding five years or both.

3.3 The process of money laundering comprises three stages, during which there may be numerous transactions that could alert a reporting institution to the money laundering activities. These stages are:

(a) **Placement:** the physical disposal of benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial system;

(b) **Layering:** the separation of benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and

(c) **Integration:** the provision of apparent legitimacy to benefits of unlawful activities. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

3.4 The illegal funds laundered through the capital market sector may be generated by unlawful activities both from outside and from within the sector. For illegal funds generated outside the sector, securities and futures transactions are used as the mechanism for concealing or obscuring the source of these funds.

4. INTERNATIONAL INITIATIVES

4.1 The Financial Action Task Force on Money Laundering (FATF) is a pre-eminent inter-governmental organization established in 1989 to examine and recommend measures to counter money laundering. The FATF's 40 Recommendations set out the framework for anti-money laundering efforts and are designed for universal application. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing.

4.2 In 1992, the International Organization of Securities Commissions ("IOSCO"), of which the Commission is a member, adopted a resolution inviting IOSCO members to consider issues relating to minimising money laundering, such as adequate customer identification, record keeping, monitoring and compliance procedures and the identification and reporting of suspicious transactions.

4.3 In June 1996, FATF issued a revised set of 40 recommendations for dealing with money laundering. The 40 Recommendations were further revised in June 2003 in response to the increasingly sophisticated combinations of techniques in laundering criminal funds. The revised 40 Recommendations apply not only to money laundering but also to terrorist financing, and when combined with the Nine Special Recommendations revised by FATF in October 2004, provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing (hereafter referred to collectively as "FATF's Recommendations").

4.4 In light of the recent work of FATF and other international organizations, IOSCO established a task force, in October 2002, to study existing securities regulatory regimes and to develop principles relating to the identification of customers and beneficial owners. IOSCO subsequently issued, in May 2004, the paper, "Principles on Client Identification and Beneficial Ownership for the Securities Industry", to guide securities regulators and regulated firms of the Malaysian capital market in implementing requirements relating to customer due diligence.

5. GENERAL PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

5.1 There is a common obligation in the AMLA requirements not to facilitate money laundering or terrorist financing. There is also a need for reporting institutions to have a system in place for reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

5.2 The AMLA requires that reporting institutions take the necessary steps in order to prevent money laundering and to report transactions if they appear to be suspicious.

The board of directors of a reporting institution should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. In seeking to comply with these requirements, reporting institutions should ensure the following:

(a) **Compliance with laws:** Reporting institutions shall ensure that laws and regulations are adhered to, that business is conducted in conformity with high ethical standards, and that service is not provided where there is good reason to suppose that transactions are associated with money laundering activities.

(b) **Co-operation with law enforcement agencies:** reporting institutions shall co-operate fully with law enforcement agencies. This includes taking appropriate measures such as timely disclosure of information by reporting institutions to the FIU and the relevant law enforcement agencies.

(c) **Policies, procedures and training:** reporting institutions shall issue and adopt policies and procedures consistent with the principles set out under the AMLA, ensure that its staff are informed of and fully understand these policies. Reporting institutions should also provide adequate training to such staff on matters provided for under the AMLA. To promote adherence to these principles, the reporting institutions shall approve and implement specific policies and procedures for customer identification, retention of financial transaction documents, and reporting of suspicious transactions.

(d) **Know Your Customer:** reporting institutions shall obtain satisfactory evidence of the customer's identity, and have effective procedures for verifying the bona fides of customers.

5.3 Each reporting institution should consider carefully the specific nature of its business, organizational structure, type of customer and transaction, etc. to satisfy itself that the measures taken by them are adequate and appropriate to follow the spirit of the suggested measures in these Guidelines.

5.4 Reporting institutions should regularly review its policies, procedures and controls to ensure its effectiveness and ensure that it is in line with international developments.

6. CUSTOMER IDENTIFICATION

6.1 Section 16 of the AMLA sets out clear customer identification requirements for reporting institutions. A reporting institution is expected to obtain satisfactory evidence of the identity and legal existence of persons applying to do business with them. Such evidence shall be substantiated by reliable documents or other means.

6.2 Reporting institutions should not keep anonymous accounts or accounts in fictitious names of their clients. Reporting institutions are required to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients when establishing business relations or conducting transactions. In this respect, reporting institutions shall:

(a) verify, by reliable means, the identity, representative capacity, domicile, legal capacity, occupation or business purpose of any person, as well as other identifying information on that person, whether he be an occasional or usual client, through the use of documents such as identity card, passport, birth certificate, driver's licence and constituent document, or any other official or private document, when establishing or conducting business relations, particularly when opening new accounts or passbooks, entering into any fiduciary transaction, or performing any cash transaction exceeding such amount as the FIU may specify; and

(b) include such details in a record.

6.3 Clients who fail to provide evidence of their identity should not be allowed to engage in business transactions with the reporting institution. Additional measures should be undertaken to determine whether to proceed with the business where initial checks fail to identify the client or give rise to suspicions that the information provided is false.

6.4 Every reporting institution shall implement and maintain appropriate guidelines for its representatives and employees to assist them in learning essential facts about their clients' backgrounds. In determining the risk profile of a particular customer or type of customers, the reporting institution should take into account, including but not limited to, the following factors:

(a) the background or profile of the customer;
(b) the nature of the customer's business;
(c) the origin of the customer (for example place of birth, residence);
(d) the customers' investment objectives;
(e) the customers knowledge and experience in dealing in securities and futures broking;
(f) the customers' financial background and where possible to be able to judge whether the amount of cash or other financial instruments going through accounts are consistent with the line of business or occupation being undertaken by the customer;
(g) for corporate customers, unduly complex structure of ownership for no good reason;
(h) means of payment as well as type of payment mode;
(i) risks associated with non face-to-face business relationships; and
(j) any other information that may suggest that the customer is of higher risk (e.g. knowledge that the customer has been refused a business relationship by another financial institution).

7. CUSTOMER DUE DILIGENCE

7.1 General

7.1.1 Reporting institutions should conduct ongoing due diligence and scrutiny of customers' identity and his / her investment objectives. This should be done

throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the reporting institutions knowledge of the customer, its business and its risk profile.

7.1.2 For clients that may require additional caution to be exercised when transacting with them, it is recommended that the activities in the clients accounts be monitored on a regular basis for suspicious transactions. One method may be to 'flag' such accounts on the reporting institutions computer. This would assist employees carrying out future transactions to take note of the 'flag' and pay extra attention to the transactions conducted on the account.

7.1.3 While extra care should be exercised in such cases, it is not a requirement that the reporting institution should refuse to do any business with such customers or automatically classify them as high risk and subject them to an enhanced customer due diligence process. Rather, reporting institutions should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering or financing of terrorism.

7.1.4 A reporting institution should consider reclassifying a customer as higher risk if, following initial acceptance of the customer, the pattern of account activity of the customer does not fit in with the reporting institutions knowledge of the customer. A suspicious transaction report should also be considered.

7.1.5 A reporting institution should not commence business relation or perform any transaction, or in the case of existing business relation, should terminate such business relation if the customer fails to comply with the customer due diligence requirements. A reporting institution should also consider lodging a suspicious transaction report with the FIU.[1]

7.2 Risk-based approach

7.2.1 The general rule is that customers are subject to the full range of customer due diligence (CDD) measures. Reporting institutions should however determine the extent to which they apply each of the CDD measures on a risk sensitive basis.

7.2.2 The basic principle of a risk-based approach is that reporting institutions adopt an enhanced CDD process for higher risk categories of customers, business relationships or transactions. Similarly, simplified CDD process is adopted for lower risk categories of customers, business relationships or transactions. The relevant enhanced or simplified CDD process may vary from case to case depending on customers' background, transaction types and specific circumstances, etc. Reporting institutions should exercise their own judgment and adopt a flexible approach when applying the specific enhanced or simplified CDD measures to customers of particular high or low risk categories.

7.2.3 Reporting institutions should establish clearly in their customer acceptance policies the risk factors for determining what types of customers and activities are to be

[1] New paragraph inserted on 15 December 2008

considered as low or high risk, while recognising that no policy can be exhaustive in setting out all risk factors that should be considered in every possible situation.

7.2.4 Apart from risk factors set out in paragraph 6.4 above for determining a customer's risk profile, the following are examples of high risk customers that a reporting institution should consider exercising greater caution when approving the opening of account and when conducting transactions for these categories of customers:

(a) Non-resident customers;
(b) Customers from locations known for its high crime rate (e.g. drug producing, trafficking, smuggling);
(c) Customers from or in countries or jurisdictions which do not or insufficiently apply the FATF Recommendations (such as jurisdictions designated as Non-Cooperative Countries and Territories (NCCT) by the FATF or those known to the reporting institution to have inadequate AML / CFT laws and regulations);
(d) Politically exposed persons (PEPs) as well as persons or companies clearly related to them;
(e) complex legal arrangements such as unregistered or unregulated investment vehicles; or
(f) companies that have nominee shareholders.

7.2.4A Upon determining a customer as "high-risk", the reporting institution should undertake enhanced CDD processes on the customer which should include:

(a) enquiring on the purpose for opening an account;
(b) enquiring the level and nature of trading activities intended;
(c) enquiring on the ultimate beneficial owners;
(d) enquiring on the source of funds;
(e) obtaining senior management's approval for opening an account; and
(f) conducting enhanced ongoing monitoring of the business relationship.[2]

7.2.5 For the purposes of paragraph 7.2.4 above, Appendix 1 sets out a non-exhaustive list of websites that may be referred to in assessing the money laundering / counter financing of terrorism risk exposure.

7.2.6 In assessing whether or not a country sufficiently applies FATF standards in combating money laundering and terrorist financing, reporting institutions should:

(a) carry out their own country assessment of the standards of prevention of money laundering and terrorist financing. This could be based on the firm's knowledge and experience of the country concerned or from market intelligence. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with a customer from the country concerned; and

(b) pay particular attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial

[2] New paragraph inserted on 15 December 2008

institutions such as the International Monetary Fund (IMF). In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, as part of their financial stability assessments of countries and territories, the IMF and the World Bank have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations.

7.2.7 Some examples of lower risk categories of customers are:

(a) financial institutions that are authorised and supervised by the SC or Bank Negara Malaysia or by an equivalent authority in a jurisdiction that is a FATF member;
(b) public companies that are subject to regulatory disclosure requirements. This includes companies that are listed on a stock exchange in a FATF member jurisdiction or on a specified stock exchange; and
(c) government or government related organisations in a non-NCCT jurisdiction where the risk of money laundering is assessed by the licensed corporation or associated entity to be low and where the licensed corporation or associated entity has no doubt as regards the ownership of the organisation.

8. RECORD KEEPING

8.1 A reporting institution shall keep a record of any transaction involving the domestic currency or any foreign currency exceeding such amount as the FIU may specify. The record shall include the following information for each transaction:

(a) the identity and address of the person in whose name the transaction is conducted, where applicable;

(b) the identity and address of the beneficiary of the person on whose behalf the transaction is conducted, where applicable;

(c) the identity of the accounts affected by the transaction, if any;

(d) the type of transaction involved, such as deposit, withdrawal, exchange of currency, cheque cashing, purchase of cashier's cheques or money orders or other payment or transfer by, through, or to such reporting institution;

(e) the identity of the reporting institution where the transaction occurred;

(f) the date, time and amount of the transaction; and

(g) the origin and the destination of the funds, where possible,

and shall also include such other information as the FIU may specify in writing.

8.2 Pursuant to section 17 of the AMLA, reporting institutions are required to prepare and maintain documentation on their clients' relationships and transactions based on the following retention periods:

(a) financial transaction documents relating to the opening of an account are to be kept for 6 years after the date of the account is closed;

(b) other financial transaction documents are to be kept for 6 years after the date on which the transactions take place or are terminated; and

(c) where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case is closed.

8.3 Reporting institutions shall retain, maintain and update documentations on their clients relationships and transactions in such a way that:

(a) the FIU, the relevant law enforcement agencies, and internal and external auditors of the reporting institution will be able to judge reliably the reporting institution's transactions and its compliance with the AMLA;

(b) any transaction effected via the reporting institution can be reconstructed; and

(c) the reporting institution can satisfy within a reasonable time any enquiry or order from the FIU or the relevant law enforcement agencies as to the disclosure of the information.

8.4 Reporting institutions should ensure that all records of clients remain up-to-date and relevant.

8.5 To achieve this, a reporting institution should consider undertaking periodic and / or ad hoc reviews of existing customer records to consider re-classifying a customer as high or low risk. The frequency for conducting these reviews should be determined based on the reporting institutions understanding of the customer and the type of relationship and transaction. For example, an appropriate time to perform an ad hoc review may be when there is a transaction that is unusual or not in line with the customer's normal trading pattern based on the reporting institutions' knowledge of the customer; when there is a material change in the way that the account is operated; when the reporting institution is not satisfied that it has sufficient information about the customer; or when there are doubts about the veracity or adequacy of previously obtained identification data.

9.0 SUSPICIOUS TRANSACTIONS

9.1 Each reporting institution shall clarify the economic background and purpose of any transaction or business relationship if its form or amount appears unusual in relation to the client, or if the economic purpose or legality of the transaction is not immediately clear. Special attention should also be paid to all complex and unusual patterns of transactions.

9.2 Suspicious transactions are likely to involve a number of factors which together raise a suspicion that the transactions may be connected with certain unlawful activities.

As a general principle, a suspicious transaction may be a transaction which causes any licensed representative or an employee of a reporting institution to have a feeling of apprehension or mistrust about the transaction considering:

(a) the nature of, or unusual circumstances, surrounding the transaction;

(b) the known business background of the person conducting the transaction;

(c) the production of seemingly false identification in connection with any transaction, the use of aliases and a variety of similar but different addresses;

(d) the behaviour of the person or persons conducting the transactions (e.g. unusual nervousness); and

(e) the person or group of persons with whom they are dealing.

9.3 If in bringing together all relevant factors, a licensed representative or an employee of a reporting institution has reasonable grounds to suspect that the transaction may be connected with certain unlawful activities, such transactions should be reported immediately to the FIU.

9.4 In the case where the compliance officer decides that there are no reasonable grounds for suspicion, the reasons for this should be fully documented by the compliance officer. He / she must also ensure that his / her decision is supported by the relevant documents and file the report.

9.5 The reporting institution must ensure that the compliance officer maintains a complete file on all internal suspicious transaction reports received by him from the reporting institutions' employees and any supportive documentary evidence irrespective of whether such reports have been submitted to the FIU.

9.6 The fact that a report may have been filed with the FIU previously should not preclude the making of a fresh report if new suspicions are aroused.

9.7 The AMLA requires reporting of a suspicious transaction as soon as practicable after forming the suspicion. The suspicion, may in some cases, be formed a considerable time after the date of the transaction as a result of additional information coming to light.

9.8 Appendix 2 lists some examples of suspicious transactions. The list is not exhaustive and only provides examples of the most basic ways in which money may be laundered through the securities and futures market.

9.9 The obligation to report is on the individual who becomes suspicious of a money laundering transaction. A licensed representative or an employee of a reporting institution who deals with customers should be made aware of the statutory obligation to report suspicious transactions. A suspicious transaction report should be made on the relevant transaction in a manner accepted by FIU.

9.10 A suspicious transaction report should be submitted using the prescribed form and forwarded to the FIU by way of mail or fax or email (password protected) or by hand. The physical forms should be placed in sealed envelope and addressed to the following:

Head of Department,
Financial Intelligence Unit,
Bank Negara Malaysia,
Jalan Dato' Onn,
50450 Kuala Lumpur
(To be opened by addressee only)

Fax no: 03-26933625

9.11 Each reporting institution is required to have in place strong reporting mechanisms for suspicious transactions. For example, the reporting institution could appoint dedicated compliance officers to maintain records and report any suspicious transactions. The reporting institution could also have an appropriate unit primarily responsible for reporting to the FIU on any suspicious transactions.

9.12 The compliance officer in a reporting institution should act as a central reference point within the organization to facilitate onward reporting to the FIU. The role of the compliance officer is not simply that of a passive recipient of ad hoc reports of suspicious transactions, but rather, he or she plays an active role in the identification and reporting of suspicious transactions, which may involve regular review of exception reports of large or irregular transactions generated by reporting institutions' internal system as well as ad hoc reports made by front-line staff. Depending on the organization structure of the reporting institution, the specific task of reviewing reports may be delegated to other staff but the compliance officer or the supervisory management should maintain oversight of the review process.

10. COMPLIANCE AND TRAINING

10.1 Pursuant to section 19 of the AMLA, a reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls to guard against and detect any offence under the AMLA. These programmes shall include:

(a) the establishment of procedures to ensure high standards of integrity of its employees or persons acting on their behalf and a screening system to evaluate the personal, employment and financial history of these employees;

(b) on-going employee training programmes, such as 'Know Your Customer' programmes, and instructing employees or persons acting on their behalf with regard to the responsibilities specified under AMLA particularly in relation to reporting of suspicious transactions to the FIU, centralisation of information, identification of clients and retention of records;

(c) an independent audit function to check compliance with such programmes; and

(d) a sound internal control system.

10.2 Employee training programmes should be conducted on a regular basis e.g. once a year, in order to ensure that employees are kept up-to-date with latest developments in this area and also as a means of ensuring that employees are reminded of their responsibilities.

10.3 A reporting institution shall also designate compliance officers at management level in each branch or in the case of a universal broker, at the designated branch, who will be in charge of the application of the internal programmes and procedures, including proper maintenance of records and reporting of suspicious transactions.

10.4 Where in the performance of his duties, a compliance officer becomes aware of any suspicious transactions, the compliance officer shall immediately report the matter to the FIU.

10.5 Notwithstanding the duties of the compliance officer, the ultimate responsibility for proper supervision, reporting and compliance pursuant to AMLA shall rest with the reporting institution and the board of directors.

10.6 Audit mechanisms may be conducted in conformity with any applicable audit standard for the detection and prevention of money laundering, to test transactions, to ensure financial transactions are following prescribed programs, rules, regulations and internal controls. The audit function may be conducted by either an external audit firm or the financial institution's internal auditor.

11.0 CONFIDENTIALITY OF REPORTING

11.1 The report is to be completed as soon as possible after the transaction and not in the presence of the subject of the report. The subject of the report must not be advised of the reporting by the reporting institution.

11.2 It is an offence to disclose to anyone that a suspicion has been formed or that information has been communicated to the FIU and the SC or to infer that these have occurred.

11.3 No civil, criminal or disciplinary proceedings shall be brought against a person who:

(a) discloses or supplies any information in any report made under the AMLA; or

(b) supplies any information in connection with such a report, whether at the time the report is made or afterwards.

11.4 No action, suit, prosecution or other proceedings shall lie or be brought, instituted, or maintained in any court or before any other authority against-

(a) the FIU or the relevant enforcement agency including the SC;

(b) any director or officer of the FIU or the relevant enforcement agency including the SC, either personally or in his official capacity; or

(c) any person lawfully acting in compliance with any direction, instruction or order of a director or officer of the FIU or the relevant enforcement agency including the SC,

for or on account of, or in respect of, any act done or statement made or omitted to be done or made, or purporting to be done or made or omitted to be done or made, in pursuance of or in execution of, or intended pursuance of or execution of the AMLA or any order in writing, direction, instruction or other thing issued under the AMLA if such act or statement was done or made, or was omitted to be done or made, in good faith.

APPENDIX 1

1. Non-Cooperative Countries and Territories
http://www.fatfgafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html

2. International Narcotics Control Strategy Report
http://www.state.gov/p/inl/rls/nrcrpt/2006/vol1/html/62102.htm

3. Transparency International 2005 Corruption Perceptions Index
http://www.transparency.org/policy_research/surveys_indices/cpi/2005

4. Office of Foreign Assets Control
http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml

5. United Nations Security Council List
http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm

APPENDIX 2

Examples of suspicious transactions:

1. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

2. The intensity of transactions for an inactive trading account suddenly increases without plausible reason.

3. Larger or unusual settlements of securities transactions in cash form.

4. 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.

5. A client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

6. Back to back deposit / loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.

7. The entry of matching buys and sells in particular securities, creating an illusion of trading. Such trading does not result in a bona fide market position, and might provide 'cover' for a money launderer.

8. In a situation where multiple accounts are used to transfer funds between accounts by generating offsetting losses and profits in different accounts.

9. Abnormal settlement instructions including payment to apparently unconnected parties.

10. A client who suddenly starts making investments in large amounts when it is known to the reporting institution that the client does not have the capacity to do so.

11. The crediting of a customers margin account using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

12. Funds credited into customer accounts from and to countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs or (ii) other criminal conduct.

13. Investors based in countries where production of drugs or drug trafficking may be prevalent.

14. Non-resident account with very large movement with subsequent fund transfers to offshore financial centers.

15. There may be circumstances where the money laundering may involve employees of reporting institutions. Hence, if there is a change in the employees' characteristics e.g. lavish lifestyles, unexpected increase in performance, etc the reporting institution may want to monitor such situations.

16. Structuring transactions to evade substantial shareholding.

17. Unusually short period of holding securities.

18. Transactions that cannot be matched with investment and income levels.