PMLA POLICY

POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING (Issued as per the requirements of the PMLA Act 2002)

These policies and procedures apply to all staff of **Chokhani Securities Limited** hereinafter referred to as "company" or "firm".

What is money laundering and terrorist financing?

Money laundering is the process by which criminals attempt to conceal the nature, location or ownership of the proceeds of their criminal activities. If they are successful in converting "dirty" money into "clean" money, the process allows them to maintain control over these proceeds and, ultimately, to provide a legitimate cover for their source of wealth. Criminal activities are not restricted just to drug trafficking or terrorist activity. Nowadays, money laundering and other related laws cover the proceeds of all crime, including organized crime, extortion, corruption, theft, fraud, criminal deception, tax evasion and many others, no matter how small.

A very wide variety of methods are used to launder money. There are no hard and fast rules as to how money laundering occurs, the only real limitations being the imagination of the money launderer and his perceptions of the risks of being caught. Methods range from passing money through a complex international web of legitimate businesses and "shell" companies, to the purchase and resale of a luxury item.

Derivatives have been used by launderers as they offer a convenient and effective way of distancing criminal proceeds from their pursuit by law enforcement. There are of course many crimes where the initial proceeds take the form of cash. However, there are also many crimes, particularly the more sophisticated ones, where cash is either not involved or has already been converted into the underlying commodities or financial instruments to which derivatives are related.

Terrorist financing can be of a very different nature. Terrorist operations frequently require only very small amounts of money and the level of sophistication of many terrorist organizations is quite low, monies being raised from "charitable" donations, levies on members of terrorist organizations, extortion rackets, etc. Others are much more sophisticated and involve real estate, underground banking, and abuse of legitimate companies and markets.

PREVENTION OF MONEY LAUNDERING ACT, 2002 AND RELEVANT STATUTORY GUIDELINES

The Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the Rules notified there under came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act.

The PMLA 2002 and rules notified thereunder impose obligation on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish information to FIU-IND. PMLA 2002 defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

Important Definitions:

1. *"intermediary" means a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992;*

2. *"proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property*

3. *"scheduled offence" means –i) the offences specified under Part A of the Schedule; or ii) offences specified under Part B of the Schedule if the total value involved in such offences is th lakh rupees or more;*

Section 3 of the Prevention of Money Laundering Act, 2002 defines offence of money laundering under:

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actua involved in any process or activity connected with the proceeds of crime and projecting it as untaint property shall be guilty of offence of money laundering.

Section 4 of the Prevention of Money Laundering Act, 2002 specifies punishment for mon laundering as under:

Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for term which shall not be less than three years but which may extend to seven years and shall also be liab to fine which may extend to five lakh rupees:

Provided that where the proceeds of crime involved in money-laundering relates to any offence specifie under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for th words "which may extend to seven years", the words "which may extend to ten years" had bee substituted."

Section 12 of the Prevention of Money Laundering Act, 2002 lays down following obligations o banking companies, financial institutions and intermediaries.

12. (1) Every banking company, financial institution and intermediary shall –

maintain a record of all transactions, the nature and value of which may be prescribed, whether suc transactions comprise of a single transaction or a series of transactions integrally connected to each othe and where such series of transactions take place within a month;furnish information of transactions referre to in clause (a) to the Director within such time as may be prescribed; verify and maintain the records of th identity of all its clients, in such a manner as may be prescribed.

Provided that where the principal officer of a banking company or financial institution or intermediary, as th case may be, has reason to believe that a single transaction or series of transactions integrally connected t each other have been valued below the prescribed value so as to defeat the provisions of this section, suc officer shall furnish information in respect of such transactions to the Director within the prescribed time. (2 The records referred to in sub-section (1) shall be maintained for a period of ten years from the date o cessation of the transactions between the clients and the banking company or financial institution o intermediary, as the case may be."

Company Policy

It is the policy of the company to prohibit and actively prevent money laundering and any activity tha facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Principal Officer Designation and Duties

The company has designated Mr.Yogesh Raja, as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the company's AML program. Mr.Yogesh Raja is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the company's compliance with AML obligations and overseeing communication and training for employees. The Principal Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND)

Written Anti Money Laundering Procedures

The Principal Officer has adopted written procedures to implement the Anti Money Laundering provisions as envisaged under the PMLA. Such procedures shall are At the time of opening an account or executing any transaction with it, the company will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under:
Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:
Identity of Client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities

CLIENT IDENTIFICATION PROCEDURE

KNOW YOUR CLIENT

The overriding principles in the identification and verification processes are Know Your Client (**"KYC"**) and Know Your Business (**"KYB"**). These principles, as well as being essential elements in combating money laundering and terrorist financing, enable Company to service its clients better. They are also essential in terms of recognition of suspicious activity. It is NOT the case that all unusual clients, transactions or circumstances need to be reported, just those that are suspicious, but it is a good place to start. It may be that upon further enquiry, the unusual elements are found to be fine, but if not, they need to be reported to Principal Officer for further consideration.

As a general rule, new client forms must be completed in relation to all new clients. Copies of identification evidence as requested on the form must be obtained as soon as possible. Independent verification of the client's identity and address should be undertaken. If it is impossible to identify the client, then he should be turned away.

In the case of corporate clients or partnerships, certified copies of incorporation documents should be obtained and at a minimum, the identity of at least one of the executive directors or equity partners should be checked in accordance with individual identification procedures. Steps should be taken to identify those with ultimate control over the company (e.g. shareholders). If possible a visit should be rendered to the potential client, as it is a good action to meet the risk face-to-face.

BEFORE THE CLIENT ACCOUNT IS OPENED

- In-person verification of all the clients is mandatory i.e. one of our employee should actually meet the ultimate client in person before accepting the documents for opening the client account and satisfy himself about the legal existence of the client.
- Each and every column of the KYC should be discussed with the client. It is mandatory that each and every column in the KYC should be filled in correctly and should be supported by adequate documents.
- The salesperson / RM to ensure that no account is opened in a fictitious name or on an anonymous basis.
- If it is not possible to ascertain the identity of the client or client is not providing the full and complete information, account of such client should not be opened.
- Extra care should be taken by the salespersons / RM while opening the accounts of the following types of clients:
    - NRI and Clients in high risk countries

- Trust, NGO or other charity organizations
- Politicians (in India or elsewhere)
- Companies who offers foreign exchange.
- Clients with dubious reputation as per public information available.

- The salesperson should enquire about the following things and satisfy himself about genuineness of the declarations made by the client in the KYC.

  - Who is the beneficial owner of the account? If the person himself is not Beneficial Owner (BO), then whether the BO is from within the family or otherwi
  - Determine on whose behalf the transaction is being conducted. If some o person is acting on behalf of client, verify the authority given by the ultimate c for acting as agent
  - Enquire about the sources of funds for making payment for the trades.

- The sales person / RM should categorize each client by assigning a risk rating viz. low medium risk and high risk. Head of Department should review the risk rating before signing the control sheet. Illustrative list of points / criteria's that should be kept in mind for assigning rating to a client are given in **Annexure I.**

FURTHER as per SEBI circular no. CIR/MIRSD/2/2013 dated January 24, 2013 that the Princ Officer will identify the Beneficial Owner and take reasonable steps to verify his identity.

A. Where the client is a person ***other than an individual or trust,*** viz., company, partnership o unincorporated association/body of individuals, the intermediary shall identify the beneficia owners of the client and take reasonable measures to verify the identity of such persons through the following information:

   a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

      Explanation: Controlling ownership interest means ownership of/entitlement to:

      i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
      ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
      iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

   b. In cases where there exists doubt under clause 4 (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

      Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

   c. Where no natural person is identified under clauses 4 (a) or 4 (b) above, the identity of the relevant natural person who holds the position of senior managing official.

B. Where the client is a ***trust,*** the intermediary shall identify the beneficial owners of

C. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

D. Intermediaries dealing with foreign investors' viz., Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued vide SEBI circular CIR/MIRSD/11/2012 dated September 5, 2012, for the purpose of identification of beneficial ownership of the client.

AFTER THE CLIENT ACCOUNT IS OPENED

- It is the responsibility of each RM to conduct scrutiny of the transactions of its clients on a daily basis and ensure that the transactions are consistent with the knowledge of RM about the client business and risk profile. Any unusual transactions should be reported to the Compliance Department or Operations Head.

- The RM's should pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose.

- The RM's should not put any restrictions on trading in any client account where an STR (Suspicious Transaction Reporting) has been made. Further, it should be ensured that there is no tipping off to the client at any level.

- Broad categories for reason for suspicion and examples of suspicious transactions are given in **Annexure II**.

The indicative list of documents required for opening an individual or non-individual account is enclosed.

INDICATIVE RESPONSIBLITIES OF SUPPORT FUNCTIONS

The roles and responsibilities of support functions / departments in implementing the policies and procedures relating to Money Laundering measures have been specified below:

ROLE OF ACCOUNT OPENING DEPARTMENT

- Any new individual client account to be compared with the list of "Banned Client List" maintained by the Account Opening Team and through www.watchoutinvestors.com. If it is a non -individual client account then names of the directors / partners / promoters / karta / authorized signatories / key management personnel should be compared.

- KYC of Trust, Charity organizations, students should be opened only with prior approval of compliance department.

- Account Opening Team should not process any new account without obtaining all the details and documents required for opening a new client account. The exceptions, if any, has to be signed off by Compliance Department.

- Checklist for account opening.

KYC and all other client related documentation by any mode should be kept for 10 years from the date of cessation of the transaction between the client and intermediary.

RISK MANAGEMENT DEPARTMENT

- The RMG team to specify internal threshold limits for each class of client accounts and p special attention to the transaction, which exceeds these limits.
- RMG to periodically check the financial details of the client accounts on large margin calls client accounts with large account equity.

FINANCE AND ACCOUNTS

- Report any Cash Transactions to Compliance Department.
- Third Party Receipts / Payments are not allowed to be accepted / made under a circumstances. If there is doubt, Principal Officer should be consulted and his advi needs to be obtained and followed.
- Records to be kept for 10 years from the date of cessation of the transaction between t client and intermediary.

NETWORKS / TECHNOLOGY

- To evolve an internal mechanism for proper maintenance and preservation of records and information in a manner that allows easy and quick retrieval of data as and when requested b the competent authorities.
- Maintain and preserve the records for the **period of ten years** from the date of cessation of the transaction between the client and intermediary.
- Hardware and technical requirements for preparing CTR and STR.
- Data files and data structures for preparing CTR and STR

INTERNAL AUDIT

Company has appointed independent Chartered Accountants Company to conduct the internal an concurrent audit of the company with basic focus on the compliance requirements of the various statute exchanges and regulators.

Internal Auditors will conduct inter alia regular audits of the company's businesses to ensure compliance with our anti-money laundering policies and procedures including the testing of systems for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

RECORD MAINTENANCE

(i) It should be ensured that the records of identification, address, account opening, and transaction are retained for the normal prescribed period or a minimum of ten years after a relationship ha ended, whichever is higher.

(ii) Records of every transaction (including vouchers) undertaken for a customer must also be retaine for the normal prescribed period or at least ten years after the transaction occurred whether th account is open or closed. These records must be sufficient to permit a transaction or series o transactions to be accurately re-created and form a reliable audit trail. This includes an transactions undertaken where settlement has been provided in cash rather than funds drawn fro the customer's account.

(iii) Records relating to training, compliance monitoring, and internal and external suspicious activity reports, should also be retained for the normal prescribed period or a minimum of ten years

(v) Documentary evidence of any action taken in response to internal and external reports o suspicious activity, including the records of the Compliance Head, must also be retained for at leas ten years. Where it is known that an investigation is ongoing, the relevant records should b retained till the investigation is completed. If there is no evidence that an investigation is underwa ten years after the external report was made, the report does not need to be retained any longer.

(vi) Where business is refused because of a failure to meet the KYC Standards or other anti-mone laundering requirements, a record of the refusal should be retained. (no record is required wher business is refused on purely commercial grounds).

ONGOING VIGILENCE – RESPONSIBILITY OF EACH AND EVERY EMPLOYEE

Employees must familiarize themselves with their customers' normal trading activities and usual mark practices in order to recognize anomalous behavior.

It is the active responsibility of each and every employee of the company to ensure that the company and i facilities, resources, employees are not being misused in any manner.

Reporting to FIU IND

For Cash Transaction Reporting

- All dealing in Cash that requiring reporting to the FIU IND will be done in the CTR format and in th matter and at intervals as prescribed by the FIU IND

For Suspicious Transactions Reporting

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of th Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This w typically be in cases where we know, suspect, or have reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade ar the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the ar requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the custom would normally be expected to engage, and we know, after examining the background, possib purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the company to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiab suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need maintain the confidentiality of the STRs

We will not notify any person involved in the transaction that the transaction has been reported, exce as permitted by the PMLA Act and Rules thereof.

AML Record Keeping

a. STR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyo outside of a law enforcement or regulatory agency or securities regulator about a STR. We w refuse any requests for STR information and immediately tell FIU IND of any such request w receive. We will segregate STR filings and copies of supporting documentation from other compa books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests other requests for STRs.

Principal Officer will be responsible to ensure that AML records are maintained properly and t
STRs are filed as required

c. Records Required
As part of our AML program, our company will create and maintain STRs and CTRs and relev
documentation on customer identity and verification. We will maintain STRs and th
accompanying documentation for at least ten years.

Training Programs

We will develop ongoing employee training under the leadership of the Principal Officer. C
training will occur on at least an annual basis. It will be based on our company's size, its custon
base, and its resources. Our training will include, at a minimum: how to identify red flags and sig
of money laundering that arise during the course of the employees' duties; what to do once the r
is identified; what employees' roles are in the company's compliance efforts and how to perfo
them; the company's record retention policy; and the disciplinary consequences (including civil a
criminal penalties) for non-compliance with the PMLA Act.
We will develop training in our company, or contract for it. Delivery of the training may inclu
educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

We will review our operations to see if certain employees, such as those in compliance, marg
and corporate security, require specialized additional training. Our written procedures will
updated to reflect any such changes.

Program to Test AML Program

a. Staffing
The testing of our AML program will be performed by the Statutory Auditors of the company

b. Evaluation and Reporting
After we have completed the testing, the Auditor staff will report its findings to the Board
Directors. We will address each of the resulting recommendations.

Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under t
supervision of the Principal Officer. We will also review the AML performance of supervisors, as part of th
annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors

Confidential Reporting of AML Non-Compliance

Employees will report any violations of the company's AML compliance program to the Principal Office
unless the violations implicate the Compliance Officer, in which case the employee shall report to th
Director, Shri Ramakant R Chokhani. Such reports will be confidential, and the employee will suffer r
retaliation for making them.

Approval

We have approved this AML program as reasonably designed to achieve and monitor our company
ongoing compliance with the requirements of the PMLA and the implementing regulations under it.

For M/s Chokhani Securities Limited

Sd/-
Ramakant R Chokhani
Director

Annexure I

BROAD CRITERIA'S FOR RISK CATEGORIZATION OF CLIENTS

High Risk Clients:

1. Trust, Charities, NGOs and organizations receiving donations.
2. Clients who are refusing to provide their financials details / source of income.
3. Non – Individual Clients having close family shareholdings or beneficial ownership i.e. less than 5 shareholders or if a single person shareholding is more 75% of the total shares.
4. Loss making Non- Individual clients or if reserves and surplus balance is less than Rs. 5 lac.
5. Clients against whom any action has been taken by SEBI/Stock Exchange or any other regulatory authority.
6. Corporate / Partnership Firms / any other entities with track record of less than 2 years.
7. Individual clients whose employer is a politician, income tax / custom department / any other government department.
8. Non Resident Indian (NRI) clients
9. Corporate clients not disclosing the identity, address of Directors, not giving financial statements.
10. Clients residing in highly sensitive areas. For example, naxalite regions, areas where dealing in narcotic drugs, immoral traffic, corruption, etc is highly predominant. This includes person residing in UAE, Chandrapur (India), Kashmir (India), Leh-Ladakh, Pakistan, Kuwait, Iran & Iraq, Bangaladesh.
11. Client having bank account with countries where secrecy of the account is maintained.
12. Politically exposed persons (PEP), family members or close relatives of PEPs. Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
13. Companies offering foreign exchange offerings.
14. Clients in high risk countries (where existence/effectiveness of money laundering ontrols is suspect or which do not or insufficiently apply FATF standards,where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent,Countries against which government sanctions are applied, countries reputed to be any of the following - Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
15. Non face to face clients.
16. Clients with dubious reputation as per public information available etc

Medium Risk Clients:

1. Individuals whose annual income ranges for last three years is Rs. 25,00,000 and above and who have not submitted any financial documents.
2. Client whose account is operated by POA holder other than Company.
3. Clients who has given trading authorization in some other person's name. (excluding sub broker)
4. House wives Accounts
5. Clients who have not given the nature of business or nature of business are lending, investment, finance, credit etc.

Low Risk Clients:

All clients not meeting the above criterions are low risk clients.

Annexu

EXAMPLES OF REASON FOR SUSPICION AND OF SUSPICIOUS TRANSACTIONS

The examples given herein below have been structured around the business processes within our indus
The list of examples is not exhaustive. The examples below should be read in the context of the partic
transaction.

The regular monitoring of all customers — both new and longstanding — must include consideration
whether accounts are being used for questionable purposes.

While it is impossible to list all the transactions or circumstances that might raise a suspicion of mo
laundering, the following questions should be closely considered:

- Is the customer willing to accept uneconomic terms without apparent reason?
- Is the transaction inconsistent with legitimate business activity?
- Is the transaction inconsistent with the normal pattern of the customer's activity?
- Is the transaction inconsistent with the customer's account-opening documents?
- Has the customer requested that the transaction be cleared in a way that is inconsistent w
  normal practice?
- Has the customer received wire transfers from, or sent wire transfers to, countries that have
  previously been associated with the customer's business?
- Is the customer or the customer's business activity associated with countries recognized
  regulators as high-risk money laundering centers?

New business

- False identification documents
- Identification documents which could not be verified within reasonable time
- A person for whom verification of identity proves unusually difficult or who is reluctant to provic
  details
- Non-face to face clients
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- A person where there are difficulties and delays in obtaining copies of meaningful accounts or othe
  documents of incorporation;
- Involvement of countries where production of drugs or drug trafficking may be prevalent, or whic
  have particular problems with organised crime, terrorism, corruption or fraud.
- A client with no discernible reason for using the firm's service (e.g. clients with distant addresse
  who could find the same service nearer their home base, or clients whose requirements are not i
  the normal pattern of the firm's business and could be more easily serviced elsewhere);
- An investor introduced by an overseas bank, affiliate or other investor, when both investor an
  introducer are based in countries where production of drugs or drug trafficking may be prevalent;

Dealing patterns

- Transactions not in line with the investor's normal trading activity / Unusual activity compared to
  past transactions.
- Buying and selling of an investment with no rationale purpose or in circumstances which appear
  unusual (e. g. churning at the client's request);
- Usually trading in low-grade securities.

- Transactions reflect likely market manipulations
- Suspicious off market transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business.
- Account used for circular trading
- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Abnormal transactions

- Involvement of apparently unrelated third parties;
- A number of transactions by the same counterparty in small amounts of the same investment and then sold in one transaction, the proceeds being credited to an account different from the original account;
- Any transaction in which the nature, size or frequency appears unusual (e. g. early termination of packaged products at a loss due to front end loading, or early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party);
- Transactions not in keeping with normal practice in the market to which they relate (e.g. with reference to market size and frequency, or at off-market prices);
- Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.
- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Large sums being transferred from overseas for making payments
- Inconsistent with the clients apparent financial standing
- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated.

Intermediaries

- There are many clearly legitimate reasons for use of an intermediary. However, the use of intermediaries also introduces further parties into transactions thus increasing complexity and preserving anonymity.
- Any apparently unnecessary use of an intermediary should give rise to further enquiry.

Employees and agents

- Changes in employee characteristics (e. g. lavish life styles or avoiding taking holidays);
- Changes in employee or agent performance (e. g. salesman has a remarkable or unexpected increase in performance);
- 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.

Payment

- A number of transactions by the same counterparty in small amounts of the same investment and then sold in one transaction;
- Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor.

Delivery

- Settlement to be made by way of bearer securities from outside a recognised clearing system;
- Allotment letters for new issues in the name of persons other than the client.
- Involvement of third parties for receipt / delivery of securities

Annexure

MONEY LAUNDERING SUSPICION REPORT FORM
FOR INTERNAL USE ONLY

Complete and send this form to Principal Officer as soon as possible.

Ref. No.:

Sr. No.	Particulars	Remarks
1.	Name and Address of Client:	
2.	Client Code:	
3.	Telephone (inc area codes):	
4.	Fax (inc area codes):	
5.	Email:	
6.	Mobile (inc area codes):	
7.	Contact Person name:	
8.	Occupation/Type of Business:	
9.	Contact details of Principal (if person not acting as Principal):	
10.	Other countries and territories involved:	
11.	Other companies and subsidiaries or persons involved:	
12.	Brief details of transaction or other circumstances:	
13.	Source of funds (if applicable):	
14.	Reasons for suspicion:	

Signed ..... Date: .....

Name:.....

TO BE COMPLETED BY MONEY LAUNDERING REPORTING OFFICER

Reported to FIU:	Yes / No
If Yes, date:	
If No, give reasons:	
Comments:	
Signed by Principal Officer	
Date:	