POLICY AND PROCEDURES ON MONEY LAUNDERING AND TERRORIST FINANCING

FY 2010-2011

INTRODUCTION

These policies and procedures apply to all staff of **FRR Shares & Securities Ltd** hereinafter referred to as "FRR".

These procedures have been introduced for two key reasons:

a) Firstly, '**FRR**' like all financial institutions is vulnerable to money laundering and terrorist financing. The risk to the reputation of '**FRR**", should it be caught up in a money laundering scheme, even incidentally, is great. '**FRR**' therefore requires all officers and staff to comply closely with these policies and procedures, as it is the policy of our company neither to participate nor otherwise assist in money laundering of any type and nature.
b) Secondly, we are required to comply with the provisions Prevention of Money Laundering Act 2002 and guidelines issues there under by various regulators from time to time.

'FRR" Anti money laundering and terrorist financing policies and procedures are designed to achieve five aims:

1. to protect the financial and operational integrity of **'FRR'** by taking all reasonable steps and exercising all due diligence to prevent use of **'FRR'** by money launderers and terrorists;
2. to protect '" and its staff and officers from unfounded allegations of money laundering and terrorist financing;
3. to avoid criminal sanctions, negative publicity or restriction of business which might otherwise follow from the involvement of **FRR** in money laundering or terrorist financing;
4. to increase **FRR**'s protection against fraud, by implementation of these policies and procedures; and
5. to comply with all relevant legislations and regulations.

Compliance with these policies and procedures is mandatory and therefore forms part of your contract of employment or director's service contract, as appropriate. Failure to comply with the spirit and / or detail of the policies and procedures is a breach of your contract and may result in disciplinary action being taken which could result in your dismissal without compensation. Further, failure to comply with elements of money laundering and terrorist financing legislation could render you personally liable to criminal prosecution, civil action and regulatory sanction.

For the reasons set out above, you will be asked to confirm your receipt and understanding of these procedures.

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 organisations is quite low, monies being raised from "charitable" donations, levies on members of terrorist organisations, extortion rackets, etc. Others are much more sophisticated and involve real estate, underground banking, and abuse of legitimate companies and markets.

Vulnerability of FRR to Money Laundering and Terrorist Financing

Certain points of vulnerability have been identified in the laundering process, which the money launderer or terrorist financier finds difficult to avoid and where his activities are more susceptible to being recognised. These are:

- establishment of new accounts;
- cross-border transactions; and
- transfers within and from the financial system.

Owing to the nature of the business FRR transacts, we will find it hard to recognise the first of these. One of the key areas to defend is in the establishment of new accounts. Accordingly, we place great emphasis on full identification and verification of applicant clients, and obtaining suitable documentary evidence. Our main protection, however, will be by keeping meticulous transaction records to enable reconstruction of audit trails.

To protect the financial and operational integrity of FRR it is vital that all staff, officers and directors, are vigilant to ensure that FRR is not unwittingly involved in money laundering or terrorist financing. All staff, officers and directors must therefore take an active role in the deterrence of money laundering, terrorist financing, and financial crime in general.

The Dangers For All of Us

Involvement in money laundering or terrorist financing can ruin individuals, institutions and even jurisdictions.

The potential dangers to you personally are:

- imprisonment;
- unlimited fines;
- destruction of reputation;
- disqualification as a director;
- termination of employment;
- civil suit.

The potential dangers for us as a company are:

- destruction of reputation;
- unlimited fines ;
- restriction, suspension or termination of our licence;
- diversion of time from business generation to crisis management;
- insolvency; and
- civil suit.

If you have any doubt or concern regarding potential incidents of money laundering or terrorist financing, or the working of the deterrence procedures, it is your responsibility to contact the Principal Officer immediately.

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) the offences specified under Part B of the Schedule if the total value involved in such offences is thirty lakh rupees or more;*

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

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

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

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

Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this

section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted."

Section 12 of the Prevention of Money Laundering Act, 2002 lays down following obligations on 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 such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;
furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;
verify and maintain the records of the 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 the case may be, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value so as to defeat the provisions of this section, such 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 of cessation of the transactions between the clients and the banking company or financial institution or intermediary, as the case may be."

INTERNAL CONTROLS

THIRD PARTY RECEIPTS ("TPR") AND PAYMENTS ("TPP")

Both TPR and TPP are considered to be high risk given that they may be used to lodge funds with FRR or pass funds through FRR as part of the laundering process. Furthermore either strategy may be used for fraud purposes or be indicative of a client who may be undertaking unauthorised investment activities on behalf of others.

Clients should not be offered or encouraged to use a TPR or TPP facility as this is contrary to FRR's policy and also a regulatory violation. If a TPR is received from a client this should be considered as suspicious and reported to the Principal Officer and Compliance Department. A request for a TPP, even on an exceptional and one-off basis will need to be justified and subject to approval. In either case the Principal Officer will decide what further action is necessary, including the involvement of law enforcement agencies.

POLITICALLY EXPOSED PERSONS ("PEPS")

These types of person are essentially senior figures with significant political influence, their immediate family members and close associates. They often have control over government funds. Should you receive enquiries from one, or someone you suspect may be one, please contact the Principal Officer for further information as to the enhanced due diligence required in relation to such people.

CASH RECEIPTS / PAYMENTS

As a policy FRR does not accept or pay cash from / to clients.

PRINCIPAL OFFICER – RESPONSIBILITIES

The company has appointed Mr. Jayesh Patel as Principal Officer for framing, updating and monitoring the internal controls, policies and procedures as per the requirements of Prevention of Money Laundering Act – 2002 (hereinafter referred to as Act).

He will be responsible for undertaking training programs and advising on money laundering issues, investigating and reporting suspicious activity to (Financial Intelligence Unit) FIU – India, Ministry of Finance.

He will determine whether the information brought to his attention gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a suspect is engaged in money laundering. He will decide whether or not a report should be made to FIU.

Principal Officer will keep a written record of all matters reported to him, of whether or not the suspicion was reported to FIU, and of the reason for his decision.

Principal Officer will also be responsible for supervising all aspects of liaison with the relevant authorities in the event of any subsequent investigation. He is responsible for establishing and maintaining adequate arrangements for awareness and training, as well as for making annual reports to senior management.

In summary, his responsibilities includes-

- Initiation and Maintenance of these procedures
- Liaison between company and the enforcement authorities
- Acting as the central point within company for receiving Money Laundering Suspicion Reports from you
- Liaison between FRR group companies and offices in money laundering related matters.

The role of Principal Officer is essentially that of co-ordination and guidance.

The primary responsibility for implementing these policies and procedures rests with each one of you personally.

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 FRR 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 the 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 the Beneficial Owner (BO), then whether the BO is from within the family or otherwise.
    - Determine on whose behalf the transaction is being conducted. If some other person is acting on behalf of client, verify the authority given by the ultimate client 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 risk, medium risk and high risk. Head of Department should review the risk rating before signing on the control sheet. Illustrative list of points / criteria's that should be kept in mind for assigning risk rating to a client are given in **Annexure I.**

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 as **Annexure IV.**

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 is enclosed herewith as **Annexure IV**

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 pay special attention to the transaction, which exceeds these limits.
- RMG to periodically check the financial details of the client accounts on large margin calls or 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 any circumstances. If there is doubt, Principal Officer should be consulted and his advise needs to be obtained and followed.

- Records to be kept for 10 years from the date of cessation of the transaction between the 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 by 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

.

RECOGNISING SUSPICIOUS ACTIVITY

For you to be able to recognize suspicious activity, you must be particularly aware of two key principles-

(a) the usual nature of the client's business (KYC - "Know Your Client"); and
(b) the usual nature of the business carried on in your business area (KYCB - "Know Your Client's Business").

Where these two principles (KYC and KYCB) do not coincide in relation to a particular transaction, the matter will certainly be unusual, and may be suspicious. What may be suspicious to you may not be suspicious to others. However, you must report all your suspicions to the Principal Officer, whether you feel that others may share your view or not. Problems with obtaining identification, verification, delays, etc, may give rise to suspicion.

Examples of what might constitute suspicious transactions are set out in Appendix 1
However, the transaction types on the list may not necessarily be suspicious, and there may be other types of transactions which you find suspicious which are not on the list.

Therefore, you must make your own mind up as to whether you think a particular transaction makes sense or not, given your knowledge of the client's business and trading objectives.

Remember that the standard of suspicion has changed and that now there is an obligation to report on an objective basis – i.e. where you should reasonably have been suspicious given the circumstances, even though you may not actually have been suspicious.

The following factors should be borne in mind:

- Is the person well known?
- Is the transaction in question is in line with the person's normal or expected activity, the financial markets in which we know him to be active, or wants to be active, and the business which he operates?
- Is the transaction is in line with normal practice in the market to which it relates, i.e., with reference to market size and frequency?
- Is the role of any agent involved in the transaction unusual?
- Is the transaction to be settled in the normal manner?
- Are there any 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?
- Are there any high risk countries or business lines involved?

REPORTING SUSPICIOUS ACTIVITY

Having become aware of suspicious or criminal activity, you must complete a FRR Money Laundering Suspicion Report Form (**see Annexure III**). If you fail to report, you may be committing a criminal offence. The golden rule is "if in doubt, report". Good faith reporting of suspicions usually carries protection from civil legal action for breach of confidentiality laws, defamation, etc., and strict restrictions are placed on revealing the identity of those making disclosures, so you should have no fear of any comeback from the suspect.

You must complete the report in as much detail as possible and report as soon as possible to Principal Officer. Do not approach the suspect if you need further information to complete the report. Instead, contact the Principal Officer who may be able to carry out such enquiries discreetly. Under NO circumstances should any money laundering matters be discussed with anyone, including other company staff, apart from Principal Officer, their deputy and legal counsel.

You may wish to discuss the matter with Principal Officer before completing the Form, in which case you may complete the form during your discussions.

DO NOT SEND THE REPORT TO THE AUTHORITIES DIRECT. THIS IS THE RESPONSIBILITY OF PRINCIPAL OFFICER. It is vital that the company co-ordinates its responses centrally in order to follow up reports properly and maintains the effectiveness of these procedures.

SUSPECT RELATIONS

You should receive an acknowledgement of your report from Principal Officer. If the Principal Officer has not responded within 2 working days you must telephone him to ensure he has received it. He may decide not to report; ask you for clarification; or report. If he does decide to report the matter to the authorities, you may or may not be told. Continue to deal with the suspect as normal until told otherwise.

Do not under any circumstances tell the suspect that you have made an internal report, or otherwise indicate to him that a report has been made or an investigation commenced.

Keep any documentation relating to the suspicion on a separate file - NOT ON THE CLIENT FILE. Do not carry out your own investigation. You are not trained or required to do so.

Refusal to carry out transactions

In most cases, reports will be acknowledged by the authorities and consent given to continue with the transaction. In exceptional circumstances, however, consent may not be given, and matters may need to be suspended, or other action taken.

INVESTIGATIONS

You are required to give Principal Officer full co-operation in relation to all investigations, providing such access to files and records as requested. If you receive requests to co-operate with law enforcement or regulatory authorities directly from them, or receive production orders, restraint orders, account monitoring orders, customer information orders, search and seizure warrants or similar court orders, you must politely refer the requesting individual to the Principal Officer and immediately inform the Principal Officer who will take care of the matter.

RECORD MAINTENANCE

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

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

(iv) Records should be maintained in such a manner that they can be easily retrieved whenever required. Records can be in any format i.e. hard, soft, on computer, or other electronic format.

(v) Documentary evidence of any action taken in response to internal and external reports of suspicious activity, including the records of the Compliance Head, must also be retained for at least ten years. Where it is known that an investigation is ongoing, the relevant records should be retained till the investigation is completed. If there is no evidence that an investigation is underway 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-money laundering requirements, a record of the refusal should be retained. (no record is required where 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 market 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 its facilities, resources, employees are not being misused in any manner.

Annexure I

BROAD CRITERIA'S FOR RISK CATEGORIZATION OF CLIENTS

High Risk Clients:

1. Trust accounts
2. Clients who are refusing to provide their financials details / source of income.
3. Non – Indivudual Clients having close family shareholdings 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. 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.

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 FRR.
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.

Annexure II

EXAMPLES OF REASON FOR SUSPICION AND OF SUSPICIOUS TRANSACTIONS

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

The regular monitoring of all customers — both new and longstanding — must include consideration of 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 money 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 with normal practice?
- Has the customer received wire transfers from, or sent wire transfers to, countries that have not previously been associated with the customer's business?
- Is the customer or the customer's business activity associated with countries recognized by 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 provide 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 other documents of incorporation;
- Involvement of countries where production of drugs or drug trafficking may be prevalent, or which 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 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 and could be more easily serviced elsewhere);

- An investor introduced by an overseas bank, affiliate or other investor, when both investor and 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.
- Trades with no economic rationale or bona fide purpose
- Doubtful sources of funds
- Appears to be a case of insider trading
- Investment proceeds transferred to a third party
- 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 III

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:	