

**Written procedures to implement the anti-money laundering provisions as envisaged under the Anti Money Laundering Act, 2002.**

The procedures shall include *inter alia*, the following three specific parameters which are related to the overall 'Client Due Diligence Process':

- (a) Policy for acceptance of clients
- (b) Procedure for identifying the clients
- (c) Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

To ensure the compliance with the above procedure, a committee named KYC Committee shall be formed constituting senior officials of the Company including at least one designated director of the Company and the Principal Officer appointed under Anti Money Laundering Act, 2002.

The customer due diligence ("CDD") measures comprise the following:

- (a) Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures.
- (b) Verify the customer's identity using reliable, independent source documents, data or information;
- (c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;
- (d) Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and
- (e) Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.
- (f) Updation of all documents, data or information of all clients and beneficial owners collected under the CDD process.

- (g) The CDD process should necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

### POLICY FOR ACCEPTANCE OF CLIENTS

This policy is being developed to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing.

The following safeguards shall be followed while accepting the clients:

- a) No account shall be opened in a fictitious / benami name or on an anonymous basis.
- b) Factors of risk perception shall be considered by verifying registered office address, correspondence addresses, nature of business activity, trading turnover etc . and manner of making payment for transactions undertaken. The clients shall be classified into low, medium and high risk categories. Clients of special category as mentioned below shall be categorized in higher category requiring higher degree of due diligence and regular update of KYC profile. Further low risk provisions should not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.
  - i. Non resident clients,
  - ii. High net-worth clients,
  - iii. Trust, Charities, NGOs and organizations receiving donations,
  - iv. Companies having close family shareholdings or beneficial ownership,
  - v. Politically exposed persons (PEP). 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 their close family members or close relatives,
  - vi. Companies offering foreign exchange offerings,
  - vii. Clients in high risk countries where existence / effectiveness of money laundering controls 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. While dealing with clients in high risk countries where existence/effectiveness of money laundering control is suspect, it is clarified that apart from being guided by the Financial Action Task

Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatfgafi.org](http://www.fatfgafi.org)), company should independently access and consider other publicly available information.

viii. Non face to face clients,

ix. Clients with dubious reputation as per public information available etc.

c) Proper documentation and other information shall be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.

d) No account shall be opened where the Company is unable to apply appropriate clients due diligence measures / KYC policies. The Company shall not continue to do business with a person with suspicious activity. in consultation with relevant authorities.

e) The persons acting for/ on behalf of the clients shall have an authority / consent letter. Adequate verification of a person's authority to act on behalf the client should also be carried out by members of KYC Committee.

f) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

#### PROCEDURE FOR IDENTIFYING THE CLIENTS

1. New clients shall have to be known to either the employees of the company or the sub-brokers.
  2. Risk management systems shall determine whether client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures should include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.
  3. Reasonable measures shall be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
  4. Each and every KYC Form received from the clients shall be placed before the KYC Committee for their approval.
3. The respective dealer / the introducer shall personally interview the clients before opening their account and be personally present in the KYC Committee Meeting to give a feedback about the clients interviewed by them.

4. Each original document should be seen prior to acceptance of a copy. Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to KYC Committee by the dealer / introducer.
5. While carrying out transactions for the client, the dealers / relationship managers shall ensure the identity of the clients by asking them relevant questions like their name and Unique client codes.
6. The Risk management shall ensure that the exposure given to clients are in conformity with the financial background of the client and in accordance with margin provided by them.
7. In cases of doubts regarding the veracity or the adequacy of previously obtained client identification data the principal officer may require the clients to submit additional documents.
8. Every year the KYC Form shall be reviewed and latest documents, if required, shall be obtained from the clients.

#### RECORD KEEPING

1. Records will be kept as per the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.
2. In order to maintain an audit trail the following information for the accounts of customers shall be kept:
  - (a) the beneficial owner of the account;
  - (b) the volume of the funds flowing through the account; and
  - (c) for selected transactions:
    - (i) the origin of the funds;
    - (ii) the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
    - (iii) the identity of the person undertaking the transaction;
    - (iv) the destination of the funds;
    - (v) the form of instruction and authority.

3. All customer and transaction records and information are available on a timely basis to the competent investigating authorities.

4. No Cash transaction with the clients will be entertained.

5. Following records shall be maintained and preserved for a period of ten years from the date of termination of an account or business relationship.

(a) All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

(b) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall also be kept for the same period.

6. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

#### MONITORING OF TRANSACTIONS

Transactions shall be monitored on a regular basis. Special attention shall be given to all complex, unusually large transactions / patterns which appear to have no economic purpose. Suspicious transactions shall also be regularly reported to the higher authorities / head of the department. Further the compliance cell of shall randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents should be made available to auditors and also to SEBI /Stock Exchanges/FIU-IND/Other relevant Authorities, during audit, inspection or as and when required.

#### TRANSACTION MONITORING AND REPORTING ESPECIALLY SUSPICIOUS TRANSACTIONS REPORTING (STR)

The following shall be reported to the Principal Officer:

- (a) Clients whose identity verification seems difficult or clients appears not to cooperate;
- (b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing/business activity;
- (c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high-risk jurisdictions;

- (d) Substantial increases in business without apparent cause;
- (e) Unusually large cash deposits, if any, made by an individual or business;
- (f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- (g) Transfer of investment proceeds to apparently unrelated third parties;
- (h) Unusual transactions by CSCs and businesses undertaken by, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.”

Further, the trading pattern of the clients shall be closely monitored by Risk Management Department to identify abnormal/suspicious exposure/position taken by the clients. No cash transactions shall be allowed except approval from Principal Officer. The Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to customer identification data and other CDD information, transaction records and other relevant information

In case, the risk management has doubts about source of funds of the client or is instigated by clients to give abnormally high exposure, the same shall be immediately reported to KYC Committee to take further action.

In case of Clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, should also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences STR will be filed If there is any reasonable grounds to believe that the transactions involve proceeds of crime.”

The Principal Officer, if thinks fit, shall report any suspicion transaction to the senior management above his next reporting level or the Board of Directors.”

In terms of the PMLA rules information relating to cash and suspicious transactions will be reported to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,  
Financial Intelligence Unit-India,  
6<sup>th</sup> Floor, Hotel Samrat,  
Chanakyapuri,  
New Delhi-110021.

Website: <http://fiuindia.gov.in>

There shall not be any restrictions on operations in the accounts where an STR has been made. Company and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. Thus, it should be ensured that there is no tipping off to the client at any level, even before, during and after the submission of an STR.