Policy for Prevention of Money Laundering Act (PMLA) / Anti Money Laundering (AML)

PART – I OVERVIEW

1. Introduction
2. Background
3. Policy and Procedures to Combat Money Laundering and Terrorist financing

PART – II DETAILED OBLIGATIONS

4. Objectives
5. Client Due Diligence (CDD)
    - 5.1 Elements of Client Due Diligence
    - 5.2 Policy for acceptance of clients
    - 5.3 Risk Based Approach
    - 5.4 Clients of special category (CSC)
    - 5.5 Client Identification Procedure
    - 5.6 Reliance on third party for carrying out Client Due Diligence (CDD)
6. Record Keeping
7. Information to be maintained
8. Retention of Records
9. Monitoring of transactions
10. Suspicious Transaction Monitoring & Reporting
11. List of Designated Individuals/Entities
12. Designation of an officer for reporting of suspicious transaction
13. Employees" Hiring/Training and Investor Education

Annexure – I
Annexure - II

1. Introduction

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities. The term "Money Laundering" is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime). It is a process of making dirty money clean. Money is moved around the financial system again and again in such manner that its origin gets hidden. Money generated from illegitimate source is converted into that derived from legitimate source. Failure to understand and deal with money laundering can lead to significant

- Regulatory risk
- Reputation risk
- Litigation risk
- Operational risk

2. Background

The PMLA came into effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on 1st July, 2005 by the Department of Revenue, Ministry of Finance and Government of India. The PMLA has been further amended vide notification dated March 6, 2009 and inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) will now be treated as a scheduled offence under schedule B of the PMLA.

As per the provisions of the PMLA, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes 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 SEBI Act , shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- All cash transactions of the value of more than Rs 10 lakh or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakh or its equivalent in foreign currency where such series of transactions take place within one calendar month.
- All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as demat account, security account maintained by the registered intermediary.

3. Policy and Procedures to Combat Money Laundering and Terrorist financing

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that 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.

4. Objectives

The objective of the AML guidelines is to prevent company from being used, intentionally or unintentionally, by criminal elements for money laundering activities.

5. Client Due Diligence

5.1 Elements of Client Due Diligence

At the time of opening an account or executing any transaction with it, the firm 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.

5.2 Policy for acceptance of clients

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in by the broker. The dealers shall accept customer strictly in accordance with the said policy:

- No account shall be opened in anonymous or fictitious / benami name(s).
- Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status Politically Exposed Persons (PEPs) etc., to enable categorization of customers into low, medium and high risk.
- The dealers shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time.

5.3 Risk Based Approach

The risk to the customer shall be assigned on the following basis:

Low Risk:

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.

Medium Risk (Level II):
Customers that are likely to pose a higher than average risk to the broker may be categorized as medium or high risk depending on customer"s background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

- Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
- Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

Risk Assessment

The Risk Assessment is required in order to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment will also consider any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

Risk Assessment is dependent on kind of customers the Company deals with.

5.4 Clients of special category (CSC): High Risk (Level III)

The dealers may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive „due diligence" for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include:

- Non Resident Customers
- High Net Worth Individuals
- Trusts, charities, NGOs and organizations receiving donations
- Companies having close family shareholding or beneficial ownership
- Firms with „sleeping partners"
- Politically Exposed Persons (PEPs)
- Those with dubious reputation as per public information available, etc.
- Companies offering foreign exchange offerings
- Clients in high risk countries

5.5 Client Identification Procedure

Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information. The dealers need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of brokering relationship. Being satisfied means that the dealer is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the dealers shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the dealers shall (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer Identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure - I for the guidance of dealers.

If the dealer decides to accept such accounts in terms of the Customer Acceptance Policy, the dealer shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure – II.

5.6 Reliance on third party for carrying out Client Due Diligence (CDD)

Company will rely on a third party subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to timefor the purpose of:

- Identification and verification of the identity of a client and (b)
- Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.

Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

6. Record Keeping

As part of our AML program, our company will create and maintain STRs and CTRs, relevant documentation on customer identity and verification as well as account files and business correspondence. We will maintain STRs and their accompanying documentation for a period of five years.

7. Information to be maintained

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- All suspicious transactions. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –
  - gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
  - appears to be made in circumstances of unusual or unjustified complexity; or
  - appears to have no economic rationale or bonafide purpose; or
  - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

The records shall contain the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

The records will be updated on daily basis, and in any case not later than 5 working days

8. Retention of Records

There is a proper mechanism for maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities.

All necessary records on transactions, both domestic and International, record of documents evidencing the identity of its clients and beneficial owners (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

All record of information related to transactions, whether attempted or executed, that are reported to FIU will be maintained for a period of five years.

9. Monitoring of transactions

The firm will monitor through the automated means of Back Office Software for unusual size, volume, pattern or type of transaction. For non automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the firm"s compliance with government reporting requirements and the firm"s AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer"s stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm"s policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs.10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm"s normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy or the customer"s activity.)
- The customer"s account shows an unexplained high level of account activity.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer"s account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the firm detects any red flag he or she will escalate the same to the Principal Officer for further investigation. 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

- Suspicious Background
  - Suspicious background or links with known criminals

- Multiple Accounts
  - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale.
  - Unexplained transfers between multiple accounts with no rationale

- Activity in Accounts
  - Unusual activity compared to past 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

- Nature of Transactions
  - Unusual or unjustified complexity
  - No economic rationale or bonafide purpose
  - Source of funds are doubtful
  - Appears to be case of insider trading
  - Investment proceeds transferred to a third party
  - Transactions reflect likely market manipulations
  - Suspicious off market transactions

- Value of Transactions
  - 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

10. Suspicious Transaction Monitoring & Reporting

For Cash Transaction Reporting (CTR)

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

For Suspicious Transactions Reporting (STR)

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This will 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 to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the any 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 customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable 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 to maintain the confidentiality of the STRs We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

11. List of Designated Individuals / Entities

At the time of account opening of the entities or individuals, name will be verified with UNSCRs list. Accounts will not be opened in the name of anyone whose name appears in said list.

12. Designation of an officer for reporting of suspicious transaction

14.1 Appointment of Principal Officer

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the broker, Senior Executive heading the Compliance Department of the broker at Corporate Office shall act as Principal Officer. He/She shall be responsible to monitor and report transactions and share information on Anti Money Laundering as required under the law. The Principal Officer shall maintain close liaison with enforcement agencies, brokers and any other institutions that are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall furnish a compliance certificate to the Board on quarterly basis certifying that Revised Anti Money laundering Policy is being strictly followed by all the dealers of the broker.

14.2 Appointment of a Designated Director

As per the PML rules, in addition to the requirement of a Principal Officer, the company has appointed Designated Director to ensure overall compliance.

13. Employees' Hiring/Training and Investor Education

15.1 Employees' Hiring

We adopt a professional and ethical hiring policy based on meritocracy. The step-by-step hiring process involves the following procedure

- Reference through known sources
- CV of the candidate is obtained with relevant information
- Screening of the candidate profile
- Call-for multi-stage interview is done
- Qualitative factor check (Basic qualitative factors such as Qualification, work experience, personal and work details are checked)
- First round of interview with dept head
- Second round with senior management
- HR verification
- Appointment letter issuance
- Confirmation of date of joining
- Doc verification (Submission of proof of evidence such as id & address proof, Bank details, Pan card and educational background credentials are obtained)
- Employee code generation and thumb impression for electronic access and attendance

15.2 Employees' Training

We will develop ongoing employee training under the leadership of the Principal Officer. Our training will occur on at least an annual basis. It will be based on our firm‟s size, its customer base, and its resources. Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employee‟s duties; what to do once the risk is identified; what employees‟ roles are in the firm‟s compliance efforts and how to perform them; the firm‟s record retention policy; and the disciplinary consequences (including civil and criminal penalties) for noncompliance with the PMLA Act.

We will develop training in our firm, or contract for it. Delivery of the training may include 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, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

15.3 Investor Education

Implementation of KYC procedures requires dealers to demand certain information from the customers that may be of personal in nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the front desk staff needs to handle such situations tactfully while dealing with customers and educate the customer of the objectives of the KYC program.

Annexure – I

Customer Identification Requirements – Indicative Guidelines

Particulars Guidelines

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The dealers should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, dealers shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, dealers should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including anyperson settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a „foundation', steps should be taken to verify the founder managers/ directors
and the beneficiaries, if defined.

Accounts of companies and firms

Dealers need to be vigilant against business entities being used by individuals as a „front" for maintaining accounts with brokers. Dealers should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.

Accounts of Politically Exposed Persons(PEPs)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a 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. Dealers should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Dealers should verify the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The dealers should seekprior approval of their concerned Heads for opening an account in the name of PEP.

Annexure-II

Customer Identification Procedure

Features to be verified and documents that may be obtained from Customers

Features Documents

Accounts of individuals

- Legal name and any other names used
  (i) UID (Aadhaar Card)
  (ii) Passport
  (iii) Voter ID
  (iv) Driving Licence
  (v) PAN Card with Photograph
  (vi) Identity Card / Document with Applicants Photo issued by various Central and state Undertaking and other institutions as per KYC form Instructions / Checklist

- Correct permanent address
  (i) Passport
  (ii) UID (Aadhaar Card)
  (iii) Voter"s Identity Card
  (iv) Ration Card
  (v) Registered Lease or Sale Agreement of Residence
  (vi) Driving licence
  (vii) Flat Maintenance Bill
  (viii) Insurance copy
  (ix) Utility Bills (Telephone, Electricity or Gas)
  (x) Bank account Statement/ Passbook
  (xi) Proof of address in the name of spouse
  (xii) Other Identity cards/ documents with Address issued by various State and Central Undertaking and other institutions as per KYC Instructions/Checklist

Accounts of companies

- Name of the company
- Principal place of business
- Mailing address of the company
- Telephone/Fax Number
  (i) Certificate of incorporation and Memorandum & Articles of Association
  (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account
  (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf
  (iv) Copy of PAN allotment letter
  (v) Copy of the telephone bill

Accounts of partnership firms

- Legal name
- Address
- Names of all partners and their addresses
- Telephone numbers of the firm and partners
  (i) Registration certificate, if registered
  (ii) Partnership deed
  (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
  (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses
  (v) Telephone bill in the name of firm/partners

Accounts of trusts & foundations

- Names of trustees, settlers, beneficiaries and signatories
- Names and addresses of the founder, the managers/directors and the beneficiaries
- Telephone/fax numbers
  (i) Certificate of registration, if registered
  (ii) Power of Attorney granted to transact business on its behalf
  (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney,
  (iv) founders/managers/ directors and their addresses
  (v) Resolution of the managing body of the foundation/association
  (vi) Telephone bill