ANTI MONEY LAUNDERING POLICY

OF

SODHANI SECURITIES LTD.

(Approved at Board Meeting held on 02nd Sep, 2022)

Applicability

This Policy is applicable for all segments including Cash, Equity Derivatives, Currency Derivatives and all other segments of National Stock Exchange of India related to SSL It also applicable for the Depository Participant (DP) Operations of SSL as DP of NSDL.

1. Introduction to PMLA

The Prevention of Money Laundering Act, 2002 (PMLA) was brought into force with effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on July 01, 2005. Subsequently, SEBI issued necessary guidelines vide circular no. ISD/CIR/RR/AML/1/06 dated January 18, 2006 and vide letter No.ISD/CIR/RR/AML/2/06 dated 20th March 2006 to all securities market intermediaries as registered under Section 12 of the SEBI Act, 1992. These guidelines were issued in the context of the recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards. SEBI has issued a comprehensive Master Circular Ref: SEBI/ HO/ MIRSD/ DO53/ CIR/ P1 2018/ 104 dated July 04, 2018 covering guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under. Compliance with these standards by all intermediaries and the country has become imperative for international financial relations.

As per the latest SEBI Master Circular, all intermediaries have an obligation to establish policies and procedures for prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. As a Registered Intermediaries we are required to:

- Issue a statement of policies and procedures, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements.
- Ensure that the content of these Directives are understood by all staff members.
- Regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures.
- Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF.
- Undertake client due diligence ("COD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction.
- Have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities.
- Develop staff members' awareness and vigilance to guard against ML and TF.

The SEBI Master Circular requires Policies and procedures to combat ML to cover the following:

- Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries.
- Client acceptance policy and client due diligence measures, including requirements for proper identification;
- Maintenance of records;
- Compliance with relevant statutory and regulatory requirements;
- Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;
- Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system 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. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors

Considering the volume & nature of business and risk profile of clients, the policy is being formulated as under:

a. Policy relating to prevention of ML and TF
b. Policy for acceptance of clients
c. Procedure for identifying the clients
d. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

General Guidelines To All Management And Operational Staff Regarding The Policy Adopted By SSL.

As per the provision of PMLA every Member shall have to

- Maintain a record of prescribed transactions,
- Furnish information of prescribed transactions to the specified authority,
- Verify and maintain records of identity of clients,
- Preserve the records for a period of five years from the date of cessation of transactions with clients.

Such transactions include:

- All cash transactions of the value of more than Rs 10 lacs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs 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 d-mat account, security account maintained by the registered intermediary.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

The Guidelines laid down the minimum requirements and it was emphasized that the intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of Money Laundering and suspicious transactions undertaken by clients.

2. Objective

The objective of this policy framework is to:

- Create awareness and provide clarity on KYC standards and AML measures.
- Outline the obligations under PMLA.
- Provide a framework for systems and procedures.
- To prevent criminal elements from using our business for money laundering activities
- To understand the customers and their financial dealings better, which in turn would help the company to manage the risk prudently
- To put in place appropriate controls for detection and reporting suspicious transactions in accordance with applicable laws/ laid down procedures

3. Scope:

These policies and procedures apply to all employees of Sodhani Securities Ltd. and are to be read in conjunction with the existing guidelines. The following procedures have been established to ensure that all employees know the identity of their customers and take appropriate steps to combat money laundering.

4. What is Money Laundering?

Money Laundering may be defined as cleansing of dirty money obtained from legitimate or illegitimate activities including drug trafficking, terrorism, organized crime, fraud and many other crimes with the objective of hiding its source and rendering it in legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process of money laundering involves creating a web of financial transactions so as to hide the origin of and true nature of these funds.

This is done in three phases – Placement Phase, Layering Phase & Integration Phase.

The first stage in the process is placement. The placement stage involves the physical movement of currency or other funds derived from illegal activities to a place or into a form that is less suspicious to law enforcement authorities

and more convenient to the criminal. The proceeds are introduced into traditional or nontraditional financial institutions or into the retail economy. The second stage is layering. The layering stage involves the separation of proceeds from their illegal source by using multiple complex financial transactions (e.g., wire t ransfers, monetary instruments) to obscure the audit trail and hide the proceeds. The third stage in the money laundering process is integration. During the integration stage, illegal proceeds are converted into apparently legitimate business earnings through normal financial or commercial operations. Having identified these stages money laundering process, financial institutions are required to adopt procedures to guard against and report suspicious transactions that occur in any stage.

5. Financial Intelligence Unit (FIU) – INDIA

The government of India set up Financial Intelligence Unit (FIU-INDIA) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.FIU-INDIA has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordination and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

6. Policy and procedures to Combat Money Laundering and Terrorist Financing of Sodhani Securities Ltd

Sodhani Securities Pvt. Ltd (SSL) has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a frame work for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to FIU as per the guidelines of PMLA Rules, 2002. Further member shall regularly review the policies and procedures on PMLA and Terrorist Financing to ensure their effectiveness.

7. Implementation of this Policy

Shri Anil Sodhani, Executive Director of SSL is the Principal Officer and Shri Anand Sodhani, Executive Director of SSL is the Designated Director as per SEBI Circular No. CIR/MIRSD /1/2014 dated 12.03.2014) responsible for compliance of the provisions of the PMLA and AML Guidelines act as a central reference point and play an active role in identification & assessment of potentially suspicious transactions. They have to ensure that SSL discharges its obligations to report suspicious transactions to the concerned authorities.

Policy for Acceptance of Clients

New clients are accepted from the following categories of persons:

- Relatives/Associates of existing Clients.
- Reference of existing Client with good trade record.
- Existing demat account holders with clean transactions.
- Walk-in clients generally not accepted.
- Delivery based clients preferred.
- Clients with reasonable financial & social status.

The following guidelines should be observed while accepting a new client:
a) No account is opened in a fictitious / benami name or on an anonymous basis. Account Opening Applications without sufficient and proper KYC documents should be rejected summarily. Application where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non genuine, or there is perceived non co-operation of the client in providing full and complete information should also be rejected and where ever such instances occur after opening the account, the account should be suspended immediately till proper compliance is made by the client.

b) **High Risk Clients**:
The following types of accounts are required to be classified as HIGH RISK CLIENTS and more care should be taken while accepting new accounts and while monitoring suspicious transactions for the purposes of PMLA reporting:

- Individual accounts (unrelated or not belonging to same family) having common address or where transactions are conducted by a one or more person for the entire group and not by the client.
- Non- individual/ Corporate accounts in different names but with common address /registered office address or correspondence addresses or with common signatories.

Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client **(KYC)** profile.

c) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

d) Special care should be taken in case of account opened/to be opened is to be operated by a means of a Power of Attorney (POA) by another person. This will include examining the authenticity of the POA submitted, independent verification from the client directly, etc. The POA should be unambiguous with relation to the authority, rights and obligation of the POA holder.

e) Accounts of persons having criminal background or of persons against whom any regulatory action has been taken by SEBI should not be opened.

Clients of special category (CSC):
The following class of clients have been listed by SEBI as Special Category Clients and special attention needs to be given while registering these class of persons as clients and while monitoring their transactions for the purpose of reporting of Suspicious transactions:
i. Non resident clients
ii. High net-worth clients,
iii. Trust, Charities, Non-Governmental Organizations (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, etc.

vi. Companies offering foreign exchange offerings
vii. Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, 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.
viii. Non face to face clients
ix. Clients with dubious reputation as per public information available etc.

SEBI Master Circular under para 2.2 has given detailed instructions for Client Due Diligence (CDD) specially in relation to non-individual entities which is reproduced below:

2.2.1 The CDD measures comprise the following:

a) Obtaining sufficient information in order to identify persons who beneficially own or control the 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 shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement

b) Verify the clients 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 client and/or the person on whose behalf a transaction is being conducted -

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

aa) 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.

bb) In cases where there exists doubt under clause (aa) 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.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

ii. For client which is a trust: Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

iii. Exemption in case of listed companies: 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.

iv. Applicability for foreign investors: Intermediaries dealing with foreign investors' may be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

v. The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of benefi d al ownership through half-yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other intermediaries, by their Board of Directors.

d) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to c).

e) Understand the ownership and control structure of the client. .

f) 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 client, its business and risk profile, taking into account, where necessary, the client's source of funds;

♑☽ Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

Client Registration / Identification Process

Client Due Diligence (CDD)
Customer Due Diligence Process entails:

- Obtaining sufficient information about to the client in order to identify who is the Actual beneficial owner of the securities or on whose behalf transaction is conducted.
- Verify the customer's identity using reliable, independent source, document, data or information.
- Conduct on-going due diligence and scrutiny of the account /client to ensure that the transaction conducted are consistent with the client's background/financial status, its activities and risk profile.
- Obtain/conduct Re-KYC documents from High Risk Clients and Special Category Clients on a yearly basis. Since Income tax Returns in India are generally filed in end September every year, this exercise would be conducted in November/December every year.
- Re-KYC of Normal Category Clients would be done once in 3 years since last update.
- Re_KYC documents would be collected in case of change of name or other demographic details like address of client, etc.

The following procedure is followed for conducting CDD:
(a) Obtain sufficient information in order to identify persons who beneficially own or control the securities trading account. The case of Companies, Bodies Corporate, Trust and Partnership firms, identity proof of persons having beneficial ownership or of the persons who ultimately own, control or influence the client transactions needs to be taken. In case of non-individual accounts, dominant share holders/list of Directors/partnership/Trustees, etc have to be obtained at the time of accepting the account.

(b) Verify the client's identity using reliable, independent source documents, data or information – currently, Income Tax website is used for verification of PAN No and identity of the client. Ministry of Corporate Affairs website http://www.mca.gov.in/MCA21/ can be used to collect information about corporate clients registered with the Registrar Of Companies in India.

(c) 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 client, its business and risk profile, taking into account, where necessary, the client's source of funds. Copies of Annual Accounts needs to be collected from Corporate Clients on a yearly basis to assess the financial position of the client.

Other operational aspects relating to client acceptance and registration are:

- New Clients are accepted only after meeting director. Credentials of the client are checked with the person referring the client. During the meeting assessment of financial position, risk appetite, investment objectives, past credentials, qualification, current working position, etc is made. Where the client is interviewed by Branch Manager (at Branches), the person interviewing the client has to be very careful and find out the clients' profile from various sources of information specially from the introducer/referrer of the client. In case of walk-in client the interviewer has to quiz the client to find out his background and obtain known some independent references to check out the client's background.
- Account is opened after receipt of completed form and after proper verification of the documents. Special care needs to be taken while verifying the documents furnished by the client with reference to his identity & address proof and financial information – bank passbook, net-worth or other financial statements furnished by the client, about their genuineness and relevance i.e. they should not be more than 3 months old.
- The officer interviewing the client has to make an objective assessment of the client as per the Policy of Client Acceptance stated above and based on the assessment has to classify the client as Normal, High Risk or Client of Special Category and the same needs to be updated in the Client's KYC documents. The officer entering the information in the back office system to create client has to ensure that the classification is properly entered in the back office system.

- Due regard is given to the provisions of Rules, Regulations, Circulars and Guidelines issued by NSE, SEBI and other Regulatory Authorities under SEBI Act, PMLA, etc relating to collection of documents and in-person verification.
- Clients under high risk profile as a matter of Company policy, should be avoided.
- The client is introduced to the dealer before accepting the order for the client is given the background of the client so that the dealer is in a proper position to analyze the capability, the risk appetite and the investment pattern of the client so that proper risk assessment can be made considering the client.
- Currently the Company is not relying on any third party for carrying out Client Due Diligence (CDD). Detailed guidelines would be framed as and when company appoints any third party for carrying on CDD.
- Accounts operated on the basis of Power of Attorney (POA) granted to Company for broking transactions: the company will accept POA from clients having trading accounts with the Company to operate the demat accounts for transfer of shares to meet the settlement obligations of shares sold by them or to meet the margin requirements. The Format of POA is enclosed with the Policy and is in consonance with the SEBI/NSDL guidelines in this regard.
- Accounts operated on the basis of Power of Attorney (POA) granted to other SEBI registered Intermediaries: currently no such account exists. When ever such an account is opened, the limits upto which the POA holder/Agent can transfer shares in single or multiple transaction on a given day has to be specified by the client.
- Accounts operated on the basis of Power of Attorney (POA) granted to entities **other than** SEBI registered Intermediaries: Clients who have granted POA should be asked to specify the limits and the circumstances in which the POA can be acted upon by the POA holder. Off-market instructions should be executed only after verifying the same with the client.

SEBI Master Circular has given detailed guidelines while dealing with PEP accounts which need to be understood and implemented thoroughly:

a) All registered intermediaries shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS. Further, the enhanced CDD measures as outlined in clause 2.2.5 shall also be applicable where the beneficial owner of a client is a PEP.

b) All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPS. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

c) Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

d) The client shall be identified by the intermediary by using reliable sources including documents/ information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

e) The information must be adequate enough to satisfy competent authorities (regulatory/ enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.

f) Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

Records & Books of Accounts

Under **The Securities Contracts (Regulation) Rules, 1957**, the following books of account and documents are required to be maintained and preserved for a period of five years:
(a) Register of transactions (Sauda book).
(b) Clients' ledger.
(c) General ledger.
(d) Journals.
(e) Cash book.
(f) Bank pass-book.
(g) Documents register showing full particulars of shares and securities received and delivered.

The following documents are required to be maintained and preserved for a period of two years:
(a) Members' contract books showing details of all contracts entered into by him with other members of the same exchange or counter-foils or duplicates of memos of confirmation issued to such other members.
(b) Counter-foils or duplicates of contract notes issued to clients.
(c) Written consent of clients in respect of contracts entered into as principals.

Under the **National Securities Clearing Corporation (Capital Market) Regulations, 1996,** the following records are required to be maintained for a period of five years:–
(a) Statements of fund and securities obligations received from the clearing(s).
(b) Record of all statements received from the settling agencies and record of all correspondence with them.
(c) Copies of all instructions obtained in writing from constituents.
(d) Records in respect of interest received on securities of constituents, monies borrowed and loaned including monies received.
(e) Records in respect of clearing charges collected separately from constituents.
(f) A Register of transaction (or other records of original entry) containing an itemized daily record of all purchases and sales of securities, showing for each such deal cleared, the name of securities, value of securities, clearing charges and name of constituents.
(g) A securities register is required to be maintained to distinguish client's securities from its own securities.

Under the National Securities Depository Limited Business Rules, 1996 the following records are required to be maintained:

16. 1. RECORDS TO BE MAINTAINED BY THE PARTICIPANTS

16.1.1. Every Participant of the Depository shall maintain the following records relating to its business for a period of five years:-

1) Delivery/Receipt Instructions given by its Clients.
2) Forms submitted by the Clients to the Participant for: -
   a) Opening of accounts with the Participant;
   b) Closing of accounts with the Participant;
   c) Freezing of accounts with the Participant;
   d) Unfreezing of accounts with the Participant.
3) Copies of correspondence from the Clients on the basis of which Clients details were updated in the DPM;
4) Record of all actions taken on the exception reports, generated by the system;
5) A register showing details of grievances received from the Clients and their present status. The following details may be specified in this regard :-
   a) name of the Client;
   b) reference number of the Client;
   c) date;
   d) particulars of complaints;
   e) actions taken by the Participant;
6) if the matter is referred to arbitration, then the particulars including the present status thereof.

7) instructions received from the Clearing Member to transfer balances from the Pool account to the Delivery account of the Clearing Member in order to enable it to meet its obligations to the Clearing Corporation;
8) instructions from the clearing member authorising the transfer of securities from the pool account of the clearing member to the accounts of its clients
9) The forms received in respect of pledge of securities;
10) The forms received in respect of transmission of securities
11) The forms received in respect of securities lending.
12) Record of serial numbers of the instruction forms for debit or pledge of securities in a Client account, issued to its Clients.

16.1.2. The following records pertaining to dematerialisation and rematerialisation of securities shall be kept by the Participants until the process of dematerialisation or rematerialisation is completed:-

- Dematerialisation request form (DRF and DRF-GS) filled by the Client;
- Certificate details of securities sent for dematerialisation;
- Proof of deliveries of DRF and securities to the Issuer or its Registrar and Transfer Agent and proof of delivery of DRF-GS and Government Securities to the Depository;
- Objection memo and certificate details of the rejected securities against the DRN;
- Rematerialisation Request Form (RRF and RRF-GS) submitted by the Client
- Proof of delivery of RRF to the Issuer or its Registrar & Transfer Agent and proof of delivery of RRF-GS to the Depository.

16.1.3. The Participant shall intimate to the Depository, the place where the above records are kept and available for audit/inspection.

16.1.4. The above requirements relating to maintenance of records shall apply not only to the records of the Participant's principal office but also any branch office and to any nominee company owned or controlled by the Participant for the purpose of conducting the business of the Participant relating to the operations of the Depository.

The following records of transactions are prescribed to be maintained under **Rule 3 of PML Rules**:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
(ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
(iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions. The records of the identity of clients have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

Records of information reported to the Director, Financial Intelligence Unit — India (FIU — IND): Records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU — IND, as required under Rules 7 and 8 of the PML Rules, shall be maintained and preserved for a period of five years from the date of the transaction between the client and the intermediary.

Operating Guidelines for use by Staff/Employees

Monitoring of transactions

1. Member regular monitors the transactions to identify any deviation in transactions/activity for ensuring effectiveness of the AML procedures.
2. Member shall pay special attention to all unusually large transactions / patterns which appears to have no economic purpose.
3. 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 shall be made available to auditors and also to SEBI/stock exchanges/FIU-IND/other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction between the client and intermediary as is required under the PMLA.

Suspicious Transactions

All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

What is a Suspicious Transaction:

Suspicious transaction means a transaction whether or not made in cash,which to a person acting in good faith -

1. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
2. Appears to be made in circumstance of unusual or unjustified complexity; or appears to have no economic rationale or bona fide purpose.

A) Reasons for Suspicious:

Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client
- Clients in high-risk jurisdiction
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- Receipt back (return) of welcome kit undelivered at the address given by the client
- Suspicious background or links with criminals.
- Clients whose identity verification seems difficult or clients that appear not to cooperate.
- Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity

The above list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances.

Suspicious Background

- Suspicious background or links with criminals

Multiple Accounts

- Large number of accounts having a common parameters such as common partners/ directors / promoters / address/ email address / telephone numbers introducer or authorized signatory
- Unexplained transfers between such multiple accounts.

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

- Source of funds is doubtful
- Appears to be case of insider trading
- Purchases made on own account transferred to a third party through an off market trans actions through DP account
- Transactions reflect likely market manipulation
- Suspicious off market transactions
- Debit or Credit transactions in a demat account through off-market, inter-depository, in a particular ISIN, through a single transaction or series of multiple transactions.
- Debit or Credit transactions due to demat, remat and pledge in a demat account, in a particular ISIN, through a single transaction or series of multiple transactions.
- Debit or Credit transaction having a high value or involving more shares which ever is samller, in an ISIN which exceeds the average size of the transaction calculated in the previous month.
- Off-market transactions where there are more transactions in an account from last fortnight.
- Any transaction in a dormant account for more shares or value which is small is considered to be suspicious.
- Off market transaction from one demat account to many other demat accounts
- Credits received in a demat account from multiple demat accounts which appear to have:
  - Unusual or unjustified complexity
  - No economic rationale or bonafide purpose
  - Source of transfer of shares are doubtful
- Purchases made on own account transferred to a third party through an off-market transaction through DP Account.

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
- Transactions appearing in FIU file from depository of a higher amount beyond financial status.

B) Policy on Identifying and Reporting suspicious transactions:

Any suspicious transaction should be immediately informed to the Executive Director in writing. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

If in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents, then all such attempted transactions should be reported in STRs, even if not completed by clients, irrespective of the amount of the transaction.

The Compliance/Principle Officer will scrutinize transactions reported in the transaction alerts generated and downloaded by NSDL on a semi-monthly basis based on the various parameters like income declared by the client (in

case of Individuals) and income and net worth (in case of non-Individuals) and the pattern of transactions observed in the preceding 6 months. In case of transactions in dormant clients, clients are contacted to confirm transaction and request for updation of KYC details is being made. The Principal Officer will review all the transactions thrown out by the filters and decides on a case-to-case basis to report to FIU with in stipulated time with complete details.

In case of broking operations, following transactions would form the basis of suspicious transactions:

1. Request for payment of Payout in cash.
2. Third party cheques requested to be credited of clients account (irrespective of the amount).
3. All payment made either by way of Demand Draft / Cheques / Money Transfer/Funds Transfer in foreign currencies irrespective of the amount. In case of DD it should be accompanied by the letter of bank in case of some unavoidable situation.
4. High Value Transactions of Clients of high risk or special category who don't give periodic disclosure of financial strength (currently a year).

C. Procedure for generation of alerts for determining suspicious transactions:

The following criteria are used to generate alerts for determining suspicious transactions for the purpose of reporting to FIU:

- Transactions reported in the PMLA Alerts file received from NSDL should be reviewed to determine suspicious transactions.
- Unusually high value Transactions in dormant accounts.
- Transactions/orders for large values placed by clients at prices far-away from the current market prices on a regular basis should be brought to the attention of the Principal Officer to check for any pattern in the placement of orders and their execution/conversion into trades. Bulk uploads made on client requests should be monitored for such orders and reported.
- Transactions of High Risk Clients/ Clients of Special Category are selected for the purpose of generating alerts.
- In case of High Risk clients, the following type of transactions are to be selected for determination
    - Offsetting transactions (if any) entered in the same security and subsequently squared up or resulting in equivalent delivery.
    - Large number of Transactions in illiquid securities in multiple accounts.
    - Transactions in illiquid securities executed between the same group clients.
    - Transactions executed far in excess of the networth resulting in huge gain/loss.

- In case of Clients of Special Category, the following type of transactions are to be selected for determination:
    - High value transactions over Rs 10.00 lacs (delivery) and Rs. 25.00 lacs (intraday square up) are selected for scrutiny.
    - Transactions in illiquid and petty stocks are to be minutely scrutinized to observe any pattern.
    - Trading volumes during a 15 day period should be compared with the average volume during the past 1 year and spikes if any needs to be noticed and evaluated for reasons.

What to Report:

- 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
- The parties to the transaction.
- The reason of suspicion.

List of Designated (debarred) Individuals/Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at http://www.un.org/sc/committees/1267/consolist.shtml. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously

scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to SEBI and FIU-IND.

Procedure for freezing of funds, financial assets or economic resources or related services

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The obligations to be followed by intermediaries to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Circular ref. no: ISD/AML/CIR-2/2009 dated October 23, 2009, which needs to be complied with scrupulously.

Para 2.9 of the SEBI Master Circular details the procedure for freezing of funds, financial assets or economic resources or related services. The same should be referred to when required.

Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:
Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

Filing of Documents/Reports with FIU-IND

The reporting requirements and formats are available on the website of FIU — IND under the Section Obligation of Reporting Entity — Furnishing Information – Reporting Format (https://fiuindia.gov.in/files/downloads/Filinq_lnformation.html). Detailed instructions/directions on the compilation and manner/procedure of submission of the reports to FIU-IND are contained in the documents. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents.

The time during which the reports are to be submitted to FIU-IND are as under:

(a) The Cash Transaction Report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.
(b) The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
(c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
(d) Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
(e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

No restrictions should be put on operations in the accounts where an STR has been made. Intermediaries and their directors, officers and employees (permanent and temporary) are 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. It is clarified that the registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, should file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

Designation of an officer for reporting of suspicious transactions

Shri Anil Sodhani, Executive Director has been appointed as the 'Principal Officer' for the purpose of implementing the various provisions of the PMLA Rules and his appointment has been informed to the Office of the Director-FIU.

Rights & Power of Principal Officer & Designated Director

1. Overall monitoring & implementation of the company's KYC/AML/CFT policy and to make changes/amendments in the PMLA/CFT policy of SSL time to time along with requirement of Record Keeping, retention, monitoring and reporting.

2. To ask details related to ultimate beneficiary ownership/person controls securities account/POA Holder /Nominee in case it seems to be suspicious.

3. To ask specific nature of its business organizational structure, income details and its way and about the nature of transaction etc of its clients and its business related entities.

4. To verify the customer identity and to refuse in opening any trading/DP account if client acceptance policy has not been met or Client has not fulfilled his due diligence measures, including requirements for proper identification and in-person verification or in case where client account has been opened in Benami name. The same refusal can be applied also based on clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions.

5. Conduct of 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. Special checks and permission for clients of special category (CSC) and transaction related to foreign exchange transaction related entities.

Verification and denial in taking the person as a client if the person is in updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) from the website http://www.un.org/sc/committees/1267/consolist.shtml.

6. To 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 SSL's knowledge of the client, its business and risk profile and the client's source of funds.

7. Stopping of the business of Intermediary in case of manipulation at its end or in providing any support to client who is engaged in any kind of manipulative trading. To approve or disapprove the mode of payment opted by the client especially in case of Cash, Demand draft, Pay order or any other mode which seems to be suspicious or crossing any regulatory limits defined.

8. Immediately stopping of Pay-in or Pay-out of funds/Securities or both if by any means the suspicious Trading pattern /wrong account information or other details has been observed.

9. Monitoring, investigation and taking action against all suspicious transactions(transactions integrally connected', 'transactions remotely connected or related) 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 SSL .

10. In handling and reporting of transactions{Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs) and Counterfeit Currency Reports (CCRs)} and sharing of information/details, as required under the law in an independent manner and Co-operation with the relevant law enforcement authorities, including the timely disclosure of information. In addition to this the maintenance of utmost confidentiality in filing of CTR and STR to FIU-IND.

11. Dealing with regulators like SEBI, FIU-INDIA or any other law enforcement agency including ministries which are involved in the fight against money laundering and combating financing of terrorism.

12. In defining the role of Internal audit/Compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system 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.

13. In conduct of any Programme/Seminar/Presentation etc. for the training of the Staff, Registered Intermediary with SSL and any other person in connection to the SSL to increase awareness and vigilance to guard against money laundering and terrorist financing.

13.3 There shall not be any restrictions on operations in the accounts where an STR has been made. Member 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. This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, member shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

Employees' Hiring/Employee's Training/ Investor Education

Hiring of Employees

The registered intermediaries should have adequate screening procedures in place to ensure high standards when hiring employees. They should identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

Employees' Training

Intermediaries must have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements should have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

Investors Education

Implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Intermediaries should prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme. Clients are also at periodic intervals informed of their obligation to provide financial and other demographic details to enable proper segregation of normal and suspicious transactions.

– xx – xx – xx – xx – xx –