SHREEYAM SECURITIES LTD. [SSL]

Policy on Prevention of Money Laundering Act

Stock Broking | Depository Participant

Version 1.8

`

INDEX		
Sr. No.	**Particulars**	**Page No.**

`

1. Introduction:-

- The Guidelines as outlined below provides a general background on the subject of money laundering and terrorist financing summarizes the main provisions of the applicable anti- money laundering and anti-terrorist financing legislation in India and provides guidance on the practical implications of the PMLA Act 2002. The Guidelines also sets out the steps that Branches / Business Associates and any of its representatives, should implement to discourage and identify any money laundering or terrorist financing activities. The relevance and usefulness of these Guidelines will be kept under review and it may be necessary to carryout amendments from time to time.

- These Guidelines are intended for use primarily by our company and its Branches / Business Associates. While it is recognized that a "one-size- fits-all" approach may not be appropriate for the securities industry in India, each Branch / Business Associates should consider the specific nature of its business, organizational structure, type of clients and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002. (PMLA).

- These Guidelines have taken into account the requirements of the Prevention of the Money Laundering Act, 2002 as applicable to the intermediaries registered under Section 12 of the SEBI Act. Some of suggested measures and procedures may not be applicable in every circumstance. Each Branch / Business Associates should consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc.

2. Background:-

- The Prevention of Money Laundering Act, 2002 has come into effect from 1st July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

- As per the provisions of the PMLA Act, 2002 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 Securities and Exchange Board of India Act, 1992) 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 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 have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.
  - 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.

3. 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.

Money Laundering could be made in three phases – 1) Placement Phase, 2) Layering Phase & 3) 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 non-traditional 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 transfers, 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.

4. Written Anti Money Laundering Procedure:-

Section 3 of PMLA has defined the "offence of money laundering" as under: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it is untainted properly shall be guilty of offence of money laundering.

Such procedures should include inter alia, the following specific parameters which are related to the overall 'Client due Diligence Process':

- Policy for acceptance of clients.
- Procedure for identifying the clients.
- Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)
- Type of Information required to be furnished.
- Time Limit prescribed by the "FIU-IND"
- Designated officer for reporting of Suspicious Transactions.
- Employee Training

5. Financial Intelligence Unit (FIU) – India:-

The government of India has 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. Policies and Procedures to Combat Money Launder And Terrorist Financing:-

The Board of 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 Policy:-

a) Team:-

Mr. Sunil Bhagaria Director of the company has been appointed as the Designated Director of the company for PMLA related activities and to supervise the work of the Anti-Money Laundering team. Under him a strong team headed by Mr. Deepika Singhvi (Principle Officer of the company) works for the implementation of the act. The Principal officer appointed would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. The Principle Officer further analyzes the data and send a report to the management, which in turn based on the recommendation of the principle officer and the compliance division head decides whether to report the suspicious transaction to the FIU or not.

b) Obligations:-

International initiatives taken to combat drug trafficking, terrorism and other organized and serious crimes have concluded that financial institutions including securities market intermediaries must establish procedures of internal control aimed at preventing and impending money laundering and terrorist financing. The said obligation on intermediaries has also been obligated under the Prevention of Money Laundering Act, 2002. In order to fulfillment these requirements, there is also a need for SEBI registered intermediaries to have a system for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

In light of the above, senior management of a registered intermediary should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The SEBI Registered Intermediaries should:

- Issue a statement of policies and procedures, on a group basis where applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements.
- Ensure that the content of these Guidelines are understood by all staff members.
- Regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review should be different from the one who has framed such policies and procedures.
- Adopt customer/ Client acceptance policies and procedures which are sensitive to the risk of money Laundering and terrorist financing.
- Undertake Client due diligence ("CDD") measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction.
- Develop staff members' awareness and vigilance to guard against money laundering and terrorist financing.

8. Client Due Diligence (CDD):-

A. The CDD measures comprise the following.

- Obtains 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. 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
- Verify the client's identity using reliable, independent source, document, data or information.
- 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.
- Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted,
- Understand the ownership and control structure of the client.
- 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;

B. Policy for acceptance of clients:

❒ For New Clients:

a) In person verification of each and every client is mandatory. Either the client should visit our office/ branch or the concerned officer should visit the client's place. And request the client to sign before the officer. Relevant stamp with proper signature of the officer is must for processing of the account.

b) Verify the PAN details on the Income Tax website.

c) Verification of Proofs with original should be properly done to avoid any manipulation. Relevant stamp with proper signature of the officer is must for processing of the account.

d) Documents like latest Income Tax returns, annual accounts, etc. should be obtained for ascertaining the financial status. If required, obtain additional information/document from the client to ascertain his background and financial status.

e) Obtain complete documentation in respect of Identity, Address, Income and bank details of the client. Without proper documentation no account should be processed. There should not be any compromise in collecting the mandatory document required to be collected as per SEBI/ PMLA guidelines while opening an account. The details of documents required should be referred from the Account Opening Master circular. Ensure that the KYC documents are properly filled up, signed and dated. Scrutinize the forms received at branch office thoroughly before forwarding it to HO for account opening.

f) Ensure that the details mentioned in the KYC matches with the documentary proofs provided and with the general verification done by us.

g) If the client does not provide the required information, then we should not open the account of such prospective clients.

h) As far as possible, a prospective client can be accepted only if introduced by existing client or associates or known entity. However, in case of walk-in clients, extra steps should be taken to ascertain the financial and general background of the client.

i) While the KYC form is collected, the officers should interview the client in respect to the sources of fund,

past experience, and kind of volume the client wants to generate.

j) We should not open any accounts in fictitious / benami / anonymous basis.

k) We should not open accounts where we are unable to apply appropriate KYC procedures.

l) A report should be submitted by the front office and in person team; this is required for initial categorization of the client.

m) KRA/ CKYC registration of the client should be checked and if the client is not registered collect all the required documents for KRA/CKYC registration.

n) KRA/CKYC registration process should be simultaneously initiated along with the account opening process.

o) Risk perception of the client need to defined having regarded to:

- Client's' location (registered office address, correspondence addresses and other addresses if applicable);
- Nature of business activity, tracing turnover etc. and
- Manner of making payment for transactions undertaken.
- The parameters of clients into Clients of special category (as given below) may be classified as higher risk and higher degree of due diligence and regular update of KYC profile should be performed.

j) Updatation of Aadhar details of the client as per the amendments of PMLA Act 2002.

❒ **For Existing Clients:**

a) Keep updating the financial status of the client by obtaining the latest Income Tax Return, Net worth Certificate, and Annual Accounts/ Annual filings made with Registrar of companies etc.

b) Update the details of the client like address, contact number, demat details, bank details etc. In case, at any point of time, we are not able to contact the client either at the address or on the phone number, contact the introducer and try to find out alternative contact details.

c) Check whether the client's identity matches 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 local enforcement / regulatory agency. For scrutiny / back ground check of the clients / HNI, websites such as www.watchoutinvestors.com should be referred. Also, Prosecution Database / List of Vanishing Companies available on www.sebi.gov.in and RBI Defaulters Database available on www.cibil.com should be checked. UNSC, 4.OFAC (Office of foreign Access and Control give by US Treasury department)

d) If a client is found matching with OFAC,UNSC or with SEBI Debarred list,we not open the account and immediately informed to Principal Officer/ Designated Director for further action.

e) Scrutinize minutely the records / documents pertaining to clients of special category (like Non-resident clients, High Net worth Clients, Trusts, Charities, NGOs, Companies having close family shareholding, Politically exposed persons, persons of foreign origin, Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange offerings, etc.) or clients from high-risk countries (like Libya, Pakistan, Afghanistan, etc.) or clients belonging to countries where corruption / fraud is highly prevalent.

f) Review the above details on a going basis to ensure that the transactions being conducted are consistent with our knowledge of clients, its business and risk profile, taking into account, where necessary, the client's source of funds.

g) Updatation of Aadhaar details of the client as per the amendment of PMLA (maintenance of records) rules 2005.

C. Risk Categorization & Acceptance of Clients through Risk-Based Approach:-

The clients may be of a higher or medium or lower risk category depending on circumstances such as the client's background, type of business relationship or transaction etc. SSL apply each of the clients due diligence measures on a risk sensitive basis. SSL adopt an enhanced client due diligence process for higher / medium / low risk categories of client. Conversely, a simplified client due diligence process may be adopted for lower risk categories of client. In line with the risk-based approach, we should obtain type and amount of identification information and documents necessarily dependent on the risk category of a particular client.

The general basis on which the clients are categorized are discussed below:-

Risk	Indicative List of clients
High Risk	1. Non-resident clients (NRI); 2. High Net worth clients (HNI) 3. Trust, Charities, NGOs and organizations receiving donations. 4. Companies having close family shareholdings or Beneficial Ownership. 5. Politically Exposed Persons (PEP) of Foreign Origin 6. Current /Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, close advisors and companies in which such individuals have interest or significant influence); 7. Companies offering Foreign Exchange offerings; 8. 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; 9. Non-face to face clients; 10. Clients with dubious reputation as per public information available etc.
Medium Risk	Individual and Non-Individual clients falling under the definition of Speculators, Day Traders and all clients trading in Futures and Options segment.
Low Risk	The clients who are not covered in the high & medium risk profile are treated as Low risk Profile client.

- **Risk Assessment**

  SSL is carry out risk assessment to identify, assess and take effective measures to mitigate any 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 shall also take into account 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 (these can be accessed at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml). The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self regulating bodies, as and when required.

D. Clients of Special Category (CSC) : Such clients shall include the following:

Such clients shall include the following:

a) Non - resident clients.

b) High net-worth clients.

c) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations.

d) Companies having close family shareholdings or beneficial ownership.

e) Politically Exposed Persons (PEP) 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.

f) Companies offering foreign exchange offerings.

a) Clients in high risk countries: Dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, intermediaries apart from being guided by the Financial Action task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to.

However, this shall not preclude intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas

b) Non face to face clients.

c) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and we should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

E. Client identification procedure (CIP):

The 'Know your Client'(KYC) policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

- SSL in compliance with the below points for Client identification procedure The client should be identified by using reliable sources including documents / information which is provided by the clients at the time of account opening. We should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship. Appropriate Risk management systems to be put in place to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic database of PEPS.
- Need to obtain senior management's 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.
- Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

- 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.
- The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the SSL in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority of the company.

SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, should frame their own internal guidelines based on their experience in dealing with their clients and legal requirements as per the established practices. Further, we should also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided. The underlying principle should be to follow the principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992 so that the intermediary is aware of the clients on whose behalf it is dealing.

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

i. The company may rely on a third party for the purpose of
   (a) 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.

ii. Such reliance shall be 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 time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

9. Records Keeping:-

To comply with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

Maintaining such records which are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries should retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

(a) The beneficial owner of the account;
(b) The volume of the funds flowing through the account; and
(c) For selected transactions:
   a) The origin of the funds;
   b) The form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
   c) The identity of the person undertaking the transaction;
   d) The destination of the funds;
   e) The form of instruction and authority.

Ensure that all client and transaction records and information are available on a timely basis to the competent

investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

In terms of rules made under the PMLA Act, Company shall maintain a record of:

a) all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
b) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
c) all cash transaction where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.;

10. Information to be maintained:-

SSL shall maintain and preserve the following information's in respect of transactions referred to in Rule 3 of PML Rules:

a) The nature of the transactions;
b) The amount of the transaction and the currency in which it is denominated;
c) The date on which the transaction was conducted; and
d) The parties to the transaction

11. Retention of Records:-

Ensure that all clients and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars. Further, the 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 between the client and intermediary.

The following document retention terms should be observed:

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

(b) Company shall maintain and preserve the records 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. (c) In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

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

However as per Securities and Exchange Board of India (Depositories And Participants) Regulations, 2018 dated 3rd October, 2018. The DP shall preserve all the original. The DP shall preserve all the original records and documents for a period of eight years. The same needs to be adhere with for DP related documents.

12. Monitoring of Transactions:-

a. Regular monitoring of transactions is requiring for ensuring effectiveness of the Anti Money Laundering procedures.

b. Special attention require to all complex, unusually large transactions / patterns which appear to have no economic purpose. Internal threshold limits to specify for each class of client accounts and pay special attention to the transaction which exceeds these limits. The background including all documents, office records/ memorandum and clarifications pertaining to such transactions and their purpose to be examined carefully and findings thereof to be recorded in writing. Such findings, records and related documents to 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 period of five years from the date of transaction between the client and the company.

c. Company shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the Company.

d. Further, the Compliance Department should 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.

Internal Alert Generation

Following Alerts to be generated as a PMLA Measure:

1. Client trading pattern
2. Trading in illiquid scrip
3. Concentration in one scrip if any,
4. Payment track record,
5. Client turnover Vs Exchange turnover.
6. Synchronised trading.
7. Client Purchase to his income/ Net worth
8. Client or group of clients dealing in common scrips
9. Whether any off-market transfers are taking place from our demat account to other Demat accounts.

Company has acquired software called "Trackwiz" from TSSL Consultancy Pvt Ltd. to monitor Suspicious Transaction as per above parameters and also to file STR's with FIU. The said software tracks all the risk & suspicious parameters suggested by SEBI and FIU authorities

13. Suspicious Transaction Monitoring & Reporting:-

For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' need to be considered

Suspicious transactions" means a transaction relating to deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical 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 an offense specified in the schedule to the act regardless of the value involved ; or

(a) Appears to be made in circumstances of unusual or unjustified complexity or

(b) Appears to have no economic rationale or bonafide purpose. or

(c) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

All the Branches/business associates shall report all Suspicious Transaction to Compliance Department immediately on observation.

On basis of the alerts generated as above / on basis of continuous monitoring, Compliance department has to furnish the information of the suspicious transactions to the Principal Officer immediately.

Whether a particular transaction is suspicious or not will depend upon the background details of the client, details of the transactions and other facts and circumstances. Followings are the circumstance, which may be in the nature of suspicious transactions: -

a) Clients whose identity verification seems difficult or clients appears not to co-operate;

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 volume without apparent cause;

e) Unusually large cash deposits 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) Off market transactions in the DP account of the clients.

i) High trading activity in the relatively illiquid scrips.

j) Major trading activity in the Z and T to T category scrips.

k) Options trading wherein client has booked unusual profit or loss which does not commensurate with the changes in the prices of underlying security in the cash segment.

l) High exposures taken by client as compared to income levels informed by clients.

m) Unusual transactions by "Client of Special category (CSCs)" and businesses undertaken by offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction need to be notified immediately to the Money Laundering Control Officer or designated Principal Officer. 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. The Principal Officer, compliance, risk and surveillance team should have timely access to client identification data, CDD information transaction records and other relevant information. The Principal Officer shall report to the Board of Directors and to the Director Operations jointly. Further the employees shall keep the fact of furnishing information in respect of transactions referred to above strictly confidential 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. It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction. 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 published by FATF on its website (wwww.fatf-gafi.org),which are categorized as "clients of Special Category" to be subjected to appropriate counter measures. Measures which include enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and application of enhanced due diligence at the time of expanding business relationships with the identified country or persons in that country to be implemented. Also steps to be taken to independently access and consider other publicly available information.

It should be ensured that irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA 2002, STR is filed if there are reasonable grounds to believe that the transactions involve proceeds of crime.

14. Due Date for reporting STR to FIU – IND:-

The Principal Officer has to furnish the information of the suspicious transactions to Director, FIU- IND within 7 working days of establishment of suspicion at the level of Principal Officer

Format

Suspicious Transaction Report in manual format has to be filed in following forms:

Description of Form	Information
Suspicious Transaction Report for an Business Associates	Details of suspicious transactions
Annexure A- Individual Detail Sheet for an Business Associates	Identification details of individual
Annexure B- Legal Person/ Entity Detail Sheet for an Business Associates (Non Individual)	Identification details of legal person /entity
Annexure C- Account Detail Sheet for an Business Associates	Details of account and transactions

15. List of Designated Individuals/ Entities:-

Maintain updated list of individuals / entities which are subject to various sanctions / measures pursuant to United Nations Security Council Resolutions (UNSCR), available from the URL http://www.un.org/sc/committees/1267/consolist.shtml. (Referred to as designated individual / entities) in electronic form. Ensure before opening any new account that the name of the proposed client does not appear in the list of designated individuals / entities.

16. Account of the client Free zed / Blocked / Restrictedfor trading on Following Circumstances:-

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 (Annexure 1) detailing the procedure for the implementation of Section 51A of the UAPA.

In view of the reorganization of Divisions in the Ministry of Home Affairs and allocation of work relating to countering of terror financing to the Counter Terrorism and Counter Radicalization (CTCR) Division, the Government has modified the earlier order dated August 27, 2009 by the order dated March 14, 2019 (Annexure 2) for strict compliance.

- Suspicious /Abnormal Trading Pattern.
- Suspected Activity, criminal activity or any legal / statutory action taken by appropriate authority against the

client /clients.

- Instructions/Directions/Orders from Regulatory Authority i.e. SEBI/RBI/Income Tax/EOW/FIU etc.
- Non Receipt of Client's Self Declaration/Documentary Evidence such as Bank Statement, ITR/Net worth certificate for due diligence.

17. Account of the client Unfreezed / Unblocked for trading on Following Circumstances:-

f) On receipt of the client's explanation and the requisite documents, the same is analyzed and taken into the consideration and records. The accounts of clients unblocked after the satisfaction of PMLA team (analyzing team) on the basis of provided document and detailed scrutiny of client's trading activity and due diligence.

18. Reporting to Financial Intelligence Unit-India:-

a) The 'Principal Officer' shall report the information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address as may modified by the SEBI from time to time:

Director, FIU-IND,
Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi – 110021 Website:
http://fiuindia.gov.in

b) Time limit prescribed for information to FIU -IND:

- The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- The Suspicious Transaction Report (STR) shall 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 shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
- The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;
- Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.
- No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.

19. Employees' Hiring/Employee's Training/ Investor Education:-

a) Hiring of Employees

There should be adequate screening procedures in place to ensure high standards when hiring employees. Key positions within our organization structure should be identified with regards 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.

b) Employees' Training

There must be an ongoing employee training program 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 guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

c) Investors Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have 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 us to sensitize clients about these requirements as the ones emanating from AML and CFT framework. We would prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT program.

20. Review Policy:-

We are reviewing the PMLA policy as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change on account of business needs and Risk Management policy.

The policy reviewed by Principal Officer & Compliance Officer and placed the changes in policy before the Board at the meeting first held after such changes are introduced and the same is communicated to all departmental heads and associate persons via email and a copy of the reviewed policy is also made available on our website.

21. Miscellaneous:-

All employees shall ensure compliance with this policy. It shall be the duty of every Employee/ Business Associate of the Company to cooperate with and provide timely disclosure and information to any inspecting authority (either internal or external) including any relevance law enforcement authorities with regard to implementation of this policy.

In addition to this policy all directives issued by SEBI/ Exchanges/ NSDL / CDSL or any other regulatory authority shall be strictly adhered to.

For Shreeyam Securities Ltd..