M/s Stratagem Stock Broker Private Limited
Reg. Off. 222,1st Floor, Subhash Nagar, Rohtak – 124001
CIN – U65999HR2006PTC036318, Email : sprintspl@gmail.com,Ph : 9215910312

PMLA POLICY

of

Stratagem Stock Broker (P) Ltd. being the member of NSEIL/BSE Ltd vide SEBI Regn Nos INZ000221434.

Policy Version No. : 1.06

Date of Last Review: 1st June 2023

Circular Ref : SEBI Master circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dt 3rd Feb 2023

POLICY FRAMEWORK FOR IMPLEMENTATION OF THE PROVISIONS OF PREVENTION AND MONEY LAUNDERING ACT (PMLA) 2002

Introduction

The Prevention of Money Laundering Act, 2002 **(PMLA)** came in force with effect from 1st July 2005.

As per the provisions of the PMLA, each market intermediary (**Reporting Entity**) (which includes a stockbroker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depositary participant, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the Securities and Exchange Board of India Act, 1992 **(SEBI Act)** shall have to adhere to client account opening procedures and maintain records of such "transactions" as prescribed by the PMLA and Rules notified there under.

Obligations of a "Reporting Entity" includes:-

a. to maintain a record of all transactions covered as per the nature and value of which may be prescribed, in such manner as to enable it to reconstruct individual transactions
b. furnish to the Partner (FIU) within such time as may be prescribed information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed
c. verify the identity of its clients in such manner and subject to such conditions as may be prescribed
d. identify the beneficial owner, if any, of such of its clients, as may be prescribed
e. maintain record of documents evidencing identity of its clients and beneficial owners, account files and business correspondence relating to its clients and information related to transactions for specified period.

For the purpose of PMLA, transactions include:

1. all cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency.
2. all series of cash transactions integrally connected to each other, which have been valued below Rs.10 Lakhs or its equivalent in foreign currency, such series of transactions within one calendar month.
3. all suspicious transactions (remotely / integrally 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 the registered intermediary.

Further, In case there is a variance in CDD/AML standards prescribed by SEBI and the regulators of the host country, branches/overseas subsidiaries of intermediaries are required to adopt the more stringent requirements of the two.

For the purpose "**Suspicions Transaction**" means a transaction whether or not ma de in cash which to a person acting in good faith:–

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bonafide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

The Anti-Money Laundering Guidelines provides a general background on the subjects of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to identify and discourage any "Money Laundering" (ML) or "Terrorist Financing" activities.

SEBI has issued various directives vide circulars, from time to time, covering issues related to Know Your Client **(KYC)** norms, Anti- Money Laundering **(AML)**, Client Due Diligence **(CDD)** and Combating Financing of Terrorism **(CFT)**. The directives lay down the minimum requirements and it is 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.

While it is recognized that a "one-size-fits-all" approach may not be appropriate for the securities industry in India, each registered intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA.

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing.

To be in compliance with these obligations, the senior management of a registered intermediary shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

The obligations of an intermediary under Prevention of Money Laundering Act, 2002 (PLMA) includes:-

a. 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;
b. ensure that the content of these Directives are understood by all staff members;
c. 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;
d. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
e. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
f. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
g. develop staff members' awareness and vigilance to guard against ML and TF.

The Policies and procedures to combat ML and TF shall cover:

a. 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;
b. Client acceptance policy and client due diligence measures, including requirements for proper identification;
c. Maintenance of records;

d. Compliance with relevant statutory and regulatory requirements;
e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
f. 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; and,
g. 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.

Accordingly, we have drafted this written policy framework (hereinafter called as "PMLA Policy") which aims to have a system in place to identify, monitor and reporting the suspected money laundering or terrorist financing transactions to law enforcing authorities within the framework of current statutory and regulatory requirements.

This policy includes the following four specific parameters which are related to the overall 'Client Due Diligence Process':

a. Policy for acceptance of clients;
b. Procedure for identifying the clients;
c. Risk Management;
d. Monitoring of Transactions.

All concerned are hereby advised to ensure that every possible measures are taken for the effective implementation of this Policy and that the measures taken are adequate, appropriate and abide by the spirit and requirements as enshrined in the PMLA.

Detailed PMLA Policy Framework

1. Principal Officer:

To ensure effective discharge of our legal obligations to report suspicious transactions to the authorities, we hereby appoint the "Principal Officer" who would act as a central reference point for the identification and assessment of potentially suspicious transactions and in facilitating onward reporting of suspicious transactions to FIU.

Complete Details of Principle Officer are as given below:-

Name : Gautam Jagga
Designation : Principal Officer/Director
Contact No : 9215910312
Email : sprintspl@gmail.com

Rights and Obligations of Principle Officer:

a. The principal office shall have all time access to customer identification data and other CDD information.
b. The principal officer shall have complete independence and authority to access and is able to report to Senior Management or his/her next reporting level or the Board of Partners.

Responsibilities:

The Principal Officer shall ensure that:

a. the Board approved PMLA Policy framework is implemented effectively.

b. systems generated data based on set parameters is regularly and promptly downloaded to analyze, identify and report transactions of suspicious nature to FIU-IND directly
c. group responds promptly to any request for information, including KYC related information maintained by us, made by the regulators, FIU-IND and other statutory authorities.
d. group`s staff members and associates are trained to address issues related to the application of the PMLA.
e. the staff selection and training process complies with the PMLA Policy.
f. group and all concerned staff is regularly updated regarding any changes / additions / modifications in PMLA provisions.

2. Appointment of Designated Partner/Director

For ensuring overall supervision and compliance with the obligations imposed under chapter IV of the Act and the Rules the group has appointed the "Designated Partner". The details of the designated Partner are as given below:-

Name : Gautam Jagga
Designation : Director
Contact No : 9813067367
Email : findgautam@gmail.com

3. Client Due Diligence Measures (CDD Measures)

The CDD measures comprise the following:

a. Obtain 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.

   For this purpose, 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 client's identity using reliable, independent source documents, data or information;

c. Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted;

   Suggestive measures for identification of **beneficial ownership** are as given below:-

   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, identification of beneficial owners of the client may be done by applying following measures namely;

   ascertain 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:

- more than 10% of shares or capital or profits of the juridical person, where the juridical person is a company;
- more than 10% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- more than 10% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

In cases where there exists doubt 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.

Where no natural person is identified under clauses mentioned 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 beneficial ownership of the client shall be identifying by taking reasonable measures to verify 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:** for dealing with foreign investors', provisions of SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client may be used as guiding principles.

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;

g. Review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data; and

h. All documents, data or information of all clients and beneficial owners collected under the CDD process shall be periodically updated.

Reliance on third party for carrying out due diligence

We may rely on a third party for the purpose of

a. identification and verification of the identity of a client and
b. where the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.

provided such third party is regulated, supervised or monitored by SEBI, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

Such reliance shall however 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 e.g.

a. we shall immediately obtain necessary information of such client due diligence carried out by the third party;
b. we shall take adequate steps to satisfy ourself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
c. we shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
d. The third party is not based in a country or jurisdiction assessed as high risk

It must always be ensured and kept in mind that as a registered intermediary, we shall be ultimately responsible for CDD and undertaking enhanced due diligence measures.

4. Policy for acceptance of Clients

Our client acceptance policies and procedures aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF so that we are in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transactions.

In nutshell the following safeguards are to be followed while accepting the clients namely;

a. No account is opened in a fictitious / benami name or on an anonymous basis.

b. Each client shall be classified into low or medium or high risk categories depending upon the risk perception.

   Such risk categorization may be arrived considering various factors of risk perception of the client having regard to:-
   - 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 undertaken.

   Clients of Special Category (CSC) (as defined later in this policy) 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 requirements and other information to be collected in respect of different classes of clients depending on the 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.

We must obtain documentary evidence of each KYC information provided by the client and verify each such supporting document with originals prior to acceptance of a copy and same be stamped “Verified with the original” and each client must be met in person before registration.

In case where online e-KYC process is being used, KYC can be completed through online / App based KYC, by carrying out in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign.

In case of e-KYC, the investor visits our website / App / digital platform and fills up the online KYC form and submits the colored copies of requisite documents online under his/her e-sign. Client`s details are cross checked using OTPs and data from PAN and Aadhar verification sites. The bank details filled by client are verified using penny drop mechanism and client s require to submit live photograph with geo tagging alongwith OVDs i.e. Client`s details are verified in following manner namely;

- Mobile and email is verified through One Time Password (OTP)
- Aadhaar is verified through UIDAIs authentication / verification mechanism, further where the investor submits his Aadhaar number, ensure that such investor to redact or blackout
- PAN is verified online using the Income Tax Database
- Bank account details are verified by Penny Drop mechanism or any other mechanism using API of the Bank.
- OVDs (such as Passport, Driving Licence, Voter Card, Proof of possession of Aadhar , NAREGA Job Card, etter issued by the National Population Register containing details of name, address etc) other than Aadhaar shall be submitted through Digiocker / under eSign mechanism

The original seen and verified requirement under SEBI circular no. MIRSD/SE/Cir-21/2011 dated October, 5 2011 for OVD would be met where the investor provides the OVD in the following manner:

- As a clear photograph or scanned copy of the original OVD, through the eSign mechanism, or;
- As digitally signed document of the OVD, issued to the Digi Locker by the issuing authority.

Further the IPV/ VIPV would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI or when the KYC form has been submitted online, documents have been provided through digi locker or any other source which could be verified online.

While carrying out VIPV, following requirements to be kept in mind:-

- The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval
- IPV shall be in a live environment, clear and still, the investor in the video shall be easily recognisable and shall not be covering their face in any manner.
- IPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP
- Photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV

The information collected by us should be enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines.

A complete identification record of person doing the In-person verification and verification of documents must be kept in readily available manner.

d. We should not open an account where we are unable to apply appropriate CDD measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided by the client is suspected to be non-genuine, or there is perceived non co-operation of the client in providing full and complete information.

   We shall not continue to do business with such a person and file a suspicious activity report. We shall also evaluate whether there is suspicious any trading in determining whether to freeze or close the account. We shall be cautious to ensure that we do not return securities or money that may be from suspicious trades.

   Further, we shall consult the relevant authorities in determining what action we shall take when we suspects suspicious trading activity.

e. We shall ensure that in case of individual client only the client himself/ herself be allowed to transact on his/her own behalf. A person may be allowed to deal on behalf of his / her spouse, dependent children or dependent parents provided a written authorization is obtained from concerned family member.

   In case of non-individual clients only the person(s) having appropriate written authorization are allowed to deal for and on behalf of the client.

   In all the cases, we must obtain the identification documents of the person so authorized to deal on behalf of the client and adequate verification of person's authority to act on behalf of the client shall also be carried out.

   The authorization letter should specify the manner in which the account shall be operated, transaction limits for the operation, additional authority (if any) required for transactions exceeding a specified quantity/value.

f. Before activating any account, we must 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.

   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.

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

   For the purpose of above and elsewhere used in this policy framework, Clients of Special Category **(CSC)** shall include:-

   i.) Non resident clients
   ii.) High net-worth clients unless known to Senior Management or introduced by a known source,
   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)** 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.) 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. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf- gafi.org), shall also independently access and consider other publicly available information.

vii.) Non face to face clients means clients who open accounts without visiting the branch/offices. Video based customer identification process is treated as face-to-face onboarding of clients

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

The above mentioned list is only illustrative and the independent judgment must be exercised to ascertain whether any other set of clients shall be classified as CSC or not.

5. Client Identification Procedures:-

Client identification procedure shall be carried out at different stages i.e. while establishing the relationship with the client, while carrying out transactions for the client or when there is any doubt regarding the veracity or the adequacy of previously obtained client identification data.

In order to ensure the compliance, we must:-

- identify whether the client or potential client or the beneficial owner of such client is a politically exposed person.

  In such cases we must seek 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.

- Senior management's prior approval is mandatory for establishing business relationships with PEPs. Further, where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, we shall obtain senior management approval to continue the business relationship.

- Reasonable measures to shall 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 obtaining adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

- Client`s information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by

us 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 shall be noted and reported to the Senior Management.

- We must follow SEBI prescribed minimum requirements relating to KYC for certain classes of registered intermediaries from time to time and conduct ongoing due diligence where inconsistencies in the information provided by the client are noticed.

- Irrespective of the amount of investment made by clients, no minimum threshold or exemption is available from obtaining the minimum information / documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of any client and non-compliance shall attract appropriate sanctions / regulatory actions.

- The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

6. **Risk-Based Approach to KYC**

Client acceptance is a critical activity in AML compliance. Registering any client means providing such client with an entry point to local and international financial systems. Client acceptance, thus, becomes the first step in controlling money laundering and terrorist financing.

Regulatory guidelines stipulate that a sound KYC program should determine the true identity and existence of the customer and the risk associated with the customer. It is therefore imperative that we capture information about their background, sources of funds, nature and type of business, domicile and financial products used by them and how these are delivered to them in order to properly understand their risk profile.

It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients.

In line with the risk-based approach, the type and amount of identification information and documents that we shall obtain necessarily depend on the risk category of a particular client and for this purpose clients may be classified into following categories namely;-

Category – A: Low Risk
Category – B: Medium Risk
Category – C: High Risk

Category "A" clients are those pose low or nil risk. These clients have a respectable and verifiable social and financial standing. Their KYC Information and financial details is easily verifiable.

Category "B" clients are those who mostly deals on intra-day basis or on speculative basis. These are the clients who maintain running account without making / withdrawing payment / deliveries frequently.

Category "C" clients are those who have defaulted in the past, have suspicious background or the clients identified as CSC.

Further, low risk profile shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

Any business relationship with "High Risk Clients" including clients identified as CSC must not be commenced unless approved by Senior Management Officials.

As customer risk rating and KYC drives enhanced due diligence and ongoing monitoring it is critical that an ongoing comprehensive assessment is conducted to understand the risks associated with our business and customers and necessary modifications and improvements in associated Client acceptance and Due Diligence Policies and Procedures are made.

Risk Assessment

We have formulated a periodic risk assessment mechanism to, identify money laundering and terrorist financing risk, assess and take effective measures to mitigate them with respect to our clients, countries or geographical areas, nature and volume of transactions, payment methods used by our 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 the URL – http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml)

Our risk assessment process consider all the relevant factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied and assessment is documented and updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

7. Transaction based Monitoring and Identification of Suspicious Transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. We can effectively control and reduce the risk only if we have an understanding of the normal and reasonable activity of the client so that we can identify deviations in transactions.

However, the extent of monitoring will depend on the risk sensitivity of the account.

Special attention is required to be given to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. We have specified internal threshold limits for each class of client accounts and do regular monitoring of the transactions which exceeds these limits.

For the purpose of monitoring of transaction under PMLA following should be taken care of:

a. examine the background and the purpose of transactions which are complex or unusually large/ with patterns which appear to have no economic purpose
b. transactions which exceed the limits specified for the relevant class of client accounts
c. understanding of normal activity in client account to identify deviations and substantial increase in business without any apparent cause
d. clients transferring large sums of money to/from overseas locations
e. attempted transfer of proceeds to unrelated 3rd parties
f. transactions of clients based in high risk jurisdictions

g. Unusual transactions by CSCs and businesses undertaken by offshore banks / financial services, businesses reported to be in the nature of export- import of small items
h. Random examination of a selection of transaction to comment on their nature

Broad category of triggers that will require the complete analysis of transaction may include:-

a. Transactions involving Artificial Volume Creation / High Value Deals / Synchronized Trades
b. client's disproportionate volume with respect to his last known financial details
c. scrip concentration-concentrated position in particular scrips which have un usual price or volumes
d. high value off market transfer instructions
e. high value transactions in a new/dormant account
f. frequent small quantity transactions in an account
g. transaction undertaken by client with respect to whom alerts raised by employees/media reports/ Enforcement Agency etc.
h. transactions undertaken by customers for whom there are adverse media reports about criminal activities/terrorist activities / terrorist financing activities
i. transaction undertaken by customers who offered false/forged identification documents / address found to be wrong

A list of circumstances which may be in the nature of suspicious transactions is given below. This 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:-

a. Clients whose identity verification seems difficult or clients that appear not to cooperate
b. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
c. Clients based in high risk jurisdictions;
d. Substantial increases in business without apparent cause;
e. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
f. Attempted transfer of investment proceeds to apparently unrelated third parties;
g. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export- import of small items.

The background including all documents/office records /memorandums/clarifications sought pertaining to identified transactions and purpose thereof shall be examined carefully and findings shall be recorded in writing.

Findings of transaction analysis must be recorded in writing, as the same along with records and related documents may required to be provided to auditors, SEBI, Stock Exchanges, FIUIND, other relevant authorities during audits or as and when asked for.

We shall apply client due diligence measures to existing clients also on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client
The compliance cell shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.
These records are required to be maintained in terms of Section 12 of the PMLA be and preserved for a period of five years from the date of transaction with the client. The 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 intermediary

8. Reporting of Suspicious Transactions

The Principal Officer would act as a central reference point in playing an active role in the identification and assessment of potentially suspicious transactions and facilitating onward reporting of suspicious transactions.
Accordingly, any potential suspicious transaction shall immediately be notified to Principal Officer which may be a detailed report with specific reference to the clients, transactions and the nature / reason of suspicion and for this purpose, transactions abandoned or aborted by clients on being asked to give some details or to provide documents are also to be reported even if not completed by clients, irrespective of the amount of the transaction.

We must ensure continuity in dealing with the reported client as normal until told otherwise and the client not be told of the report/suspicion i.e. group officials and employees shall be prohibited from "Tipping off" the fact that a STR or related information is being reported or provided to the FIU-IND.

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 shall examine the transaction in details and if reaches to the conclusion that the notified transaction is "Suspicious" shall report the same to **Financial Intelligence Unit** (FIU) within 7 days from the date of arriving at such conclusion by filing the Suspicion Transaction Report (STR).

It is clarified that the STR must be filed irrespective of the amount of transaction and/or the threshold limit, if there are reasonable grounds to believe that the transactions involve proceeds of crime.

The 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, shall be categorised as 'CSC'. Such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

9. Information to be maintained

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

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it is denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction

10. Record Keeping

We, as an SEBI registered Intermediary, shall maintain all the records to ensure compliance of requirements contained in SEBI Act 1992, Rules and Regulations made there under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

We are required to maintain such records as 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 behaviour.

In case of any suspected 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 shall 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:
    i. the origin of the funds
    ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc
    iii. the identity of the person undertaking the transaction;
    iv. the destination of the funds;
    v. the form of instruction and authority.

We shall 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, we 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 thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

We shall ensure maintaining proper record of transactions prescribed under Rule 3 of PML Rules) namely;-

a. all cash transactions of the value of more than rupees ten lakh 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;

    It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered;
c. all cash transactions 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 including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the registered intermediary

Records to be maintained in a way that all client and transaction records and information are available on a timely basis to the competent investigating authorities.

11. Retention of Records

We shall ensure Internal mechanism for proper maintenance and preservation of records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities

Following Document Retention Terms should be observed:

a. the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of **FIVE YEARS (5)** from the date of transactions with the client.
b. Records evidencing the identity of clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of **FIVE**

YEARS (5) after the business relationship between a client has ended or the account has been closed, whichever is later

c. In situations where the records relate to on-going investigation 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. All necessary records 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, shall be maintained and preserved for a period of **FIVE YEARS (5)** from the date of the transaction with the client

Records may be maintained in both hard and / or soft copies.

12. Employees Hiring

We have adequate screening procedures in place to ensure high standard when hiring employees. We have identified the key positions within the Company structure having regard to the risk of money laundering and terrorist financing and the size of our business. We shall ensure that the employees taking up such key positions are suitable and competent to perform their duties

The HR Department is instructed to verify the identity, cross check all the references, family background and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.

The department should obtain the following documents:

1. Photographs
2. Proof of address
3. Identity proof
4. Proof of Educational Qualification
5. Proof of Bank Account Details

13. Training of staff/Employees

All the staff members involved in front office dealings, back office, KYC & Compliances, Risk Management or any kind of client dealings (including the APs and their dealing staff) need to be adequately trained in AML and CFT (Combating Financing of Terrorism) procedures. They should fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of our systems being misused by unscrupulous elements.

Accordingly, we have an ongoing employee-training programme (in-house as well as sending employees for attending of independent training workshops) so that the concerned staff are adequately trained in AML and CFT procedures. These training programs are conducted on periodic basis and each of the concerned staff is required to attend atleast 2 such training programs each year.

Further, the Principle Officer is authorized to ensure that all the concerned staff is well versed with latest modifications in the PMLA policy framework and is adequately sensitized to the risks of ML & TF.

14. Investor' Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have 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 clients with regard to

the motive and purpose of collecting such information. We, therefore need to sensitize prospective client that these requirements emanating from AML and CFT framework.

This may either be done by preparing specific literature or by educating the clients/sub-brokers/Authorised Person on the objectives of the Anti Money Laundering (AML) / Combating Financing of Terrorism (CFT) programme.

15. Review of PMLA/CFT Procedures

The policy shall be reviewed periodically so as to incorporate the latest change(s) in the Anti Money Laundering Act 2002 or change in any other act, bye-lows, rules, regulations of SEBI, CBI or in any statutory and regulatory government department related to or affect to this.

Further the review of this policy framework shall be undertaken by the person other than the one who has framed this policy.

16. 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 Act and amendment thereto. In terms of said regulations, we as an intermediary have to ensure that we do not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2).

WRITEUP ON "PREVENTION OF ANTI MONEY LAUNDERING ACT 2002" FOR THE INFORMATION OF CUSTOMERS

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.

The purpose of this act is to prevent financing of terrorism and to prevent laundering of money i.e. to legalize or channelize the money generated from illegal activities like drug trafficking, organized crimes, hawala rackets and other serious crimes.

The PMLA are applicable to all intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under Section 12 of the SEBI Act.

All these entities 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:

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

It is the obligation of an Intermediary to report certain kind of transactions routed through them to FINANCIAL INTELLEGENCE UNIT (FIU) – INDIA a department specially set up to administer this Act under the Ministry of Finance.

Any such type of transaction, though not executed but attempted and failed are also required to be reported.

In order to comply with the provisions of the Act, we as an intermediary need to:-

a. Obtain sufficient information in order to identify persons who beneficially own or control the securities account.
b. Verify the client's identity using reliable, independent source documents, data or information;
c. Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted
d. Verify the identity of the beneficial owner of the client
e. Conduct ongoing due diligence and scrutiny

f. Periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process
g. No account is open in a fictitious / benami name or on an anonymous basis
h. Ensure that no account is opened where the we are unable to apply appropriate CDD measures / KYC policies or where client`s identity verification seems difficult or client appears not to co-operate.

It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. The basic principle enshrined in this approach is that an enhanced client due diligence process is required for higher risk categories of clients. Such clients shall include:-

i. Clients of Special Category i.e.
   - Non Residents
   - HNIs
   - Trust, Charities, NGOs and organizations receiving donations
   - Companies with close family holdings or beneficial Ownership
   - Politically Exposed Persons
   - Companies offering foreign exchange offerings
   - Clients in high risk countries
   - Non face to face clients
   - Clients with dubious reputation as per public information available etc

ii. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash

iii. Attempted transfer of investment proceeds to unrelated third parties

It may be noted that no account trading / demat can be opened in the name of entities whose name appear in the list of UNSC or entities debarred by SEBI.

The end clients are therefore advised to co-operate with us by providing additional information / documents if asked at the time to opening of the account and / or for during the course of dealings with us to ensure due compliance of the requirements under the PMLA Act.

As a responsible citizen it is our statutory as well as moral duty to be vigilant and refrain from temptation of easy monetary gains by knowingly or unknowingly supporting the people who are involved in activities which are endangering our freedom and causing damage to nation and to us as well.

For any further clarification, you may please refer to detailed PMLA Policy published on our website or contact Principal Office of the company.

Lists of Red Flag Indicators for Terrorist Financing – FIU

a. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
b. Management appears to be acting according to instructions of unknown or inappropriate person(s). Unnecessarily complex client structure.
c. The client is reluctant to provide all the relevant information or the accountant has reasonable doubt that the provided information is correct or sufficient.
d. Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
e. Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
f. Client starts or develops an enterprise with unexpected profile or early results. Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
g. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
h. Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
i. Investment in real estate at a higher/lower price than expected.
j. Large international payments with no business rationale. Unusual financial transactions with unknown source.
k. Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.
l. Clients incorporated in countries that permit bearer shares. Over and under invoicing of goods/services.
m. Multiple invoicing of the same goods/services.
n. Falsely described goods/services –Over and under shipments (e.g. false entries on bills of lading).
o. Misuse of pooled client accounts or safe custody of client money or assets. Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures).
p. Misuse of introductory services, e.g. to financial institution

Four Lists of Red Flag Indicators for Terrorist Financing by FIUs of other Countries

A. Financial and behavioural Indicators Published by The Egmont Group of Financial Intelligence Units

Indicators linked to the financial transactions:

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
4. Transactions which are inconsistent with the account's normal activity.
5. Deposits were structured below the reporting requirements to avoid detection.
6. Multiple cash deposits and withdrawals with suspicious references.
7. Frequent domestic and international ATM activity.
8. No business rationale or economic justification for the transaction.
9. Unusual cash activity in foreign bank accounts.
10. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
11. Use of multiple, foreign bank accounts.

Behavioural Indicators:

1. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.
3. Inclusion of the individual in the United Nations 1267 Sanctions list.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family member or third party accounts.
7. Use of false identification.
8. Abuse of non-profit organization.

B. Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual

Activity Inconsistent with the Customer's Business:

a. Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
b. The stated occupation of the customer is not commensurate with the type or level of activity.
c. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
d. Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
e. A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
f. Funds Transfers:
g. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
h. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
i. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
j. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
k. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
l. Other Transactions That Appear Unusual or Suspicious:
m. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
n. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
o. A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
p. Banks from higher-risk locations open accounts.
q. Funds are sent or received via international transfers from or to higher-risk locations.
r. Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

C. Financial Red Flags Published by DML Associates LLC:

1. IP logins in areas of conflict such as near the Syrian border, to include Jordan and Lebanon, but particularly in Turkey
2. Periods of transaction dormancy, which could be the result of terrorist training or engagement in combat
3. ATM cash withdrawals in areas of conflict
4. Wire transfers to areas of conflict
5. Charitable activity in areas of conflict especially in Syria
6. Financial activity identifiable with travel [purchase of airline tickets] to Syria through Turkey and other points of entry to include Jordan, Lebanon and Israel

D. Terrorist Activity Financing Related Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)

It may be noted that a single indicator on its own may seem insignificant, but combined with others, could provide reasonable grounds to suspect that the transaction is related to terrorist financing activity.

1. Client accesses accounts, and/or uses debit or credit cards in high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
2. Client identified by media or law enforcement as having travelled, attempted/intended to travel to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
3. Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
4. The client mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
5. Client depletes account(s) by way of cash withdrawal.
6. Client or account activity indicates the sale of personal property/possessions.
7. Individual/Entity's online presence supports violent extremism or radicalization.
8. Client indicates planned cease date to account activity.
9. Client utters threats of violence that could be of concern to National Security/Public Safety.
10. Sudden settlement of debt(s) or payments of debts by unrelated 3rd party(ies).
11. Law enforcement indicates to reporting entity that the individual/entity may be relevant to a law enforcement and/or national security investigation.
12. Client's transactions involve individual(s)/entity(ies) identified by media or law enforcement as the subject of a terrorist financing or national security investigation.
13. Client donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).
14. Client conducts uncharacteristic purchases (e.g. camping/outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).
15. A large number of email transfers between client and unrelated 3rd party(ies).
16. Client provides multiple variations of name, address, phone number or additional identifiers.
17. The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

The red flags indicators noted above can conveniently be shared with staff to create the awareness amongst them for tracking and reporting suspicious transactions and for enhancing the efforts to counter terrorism.