PMLA POLICY

Of the Group comprising of

Raghunandan Capital (P) Ltd.

Being the Member of NSEIL vide SEBI Regn. No INZ000307234,
Being the Member of BSE Ltd. vide SEBI Regn. No INZ000307234,
Being the Member of MSEI Ltd. vide SEBI Regn. No INZ000307234

And

Depository Participant of CDSL vide SEBI Regn. No IN-DP-213-2016

Policy Version No. **3.07**

Date of Last Policy Review: **28TH MAY 2025**

Reference: SEBI Master Cir- SEBI/ HO/ MIRSD/ DOS3/ CIR/ P/ 2018/104 Dt. 04/07/2018 and Circulars issued thereafter.

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 Director (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 made 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 is required to implement suggested measures and procedures considering the specific nature of its business, organizational structure, type of clients and transactions, etc. to ensure that they are effectively applied.

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. issuance and adoption of written policy statement, on a group basis(wherever applicable), for dealing with the risk of MF and TF within the framework of current statutory and regulatory requirements,
b. ensuring that these directives and contents of policy is understood by all staff members,
c. regular review of policy and procedures of prevention of ML & TF and to ensure that such reviews are conducted by the person other that the one framing the policy,
d. adoption of client acceptance policies and procedures which are sensitive to the risk of MF & TF,
e. undertaking client due diligence measures to an extent that is sensitive to the risk of ML & TF
f. compliance with relevant statutory and regulatory requirements
g. have system in place for identification, monitoring and reporting of suspected ML and TF transactions to concerned authorities
h. co-operation with relevant law enforcement authorities and timely disclosure of information
i. defining the role of internal auditors to ensure compliance of policies, procedures and control to prevent money laundering.

Accordingly, we have drafted this written policy framework (hereinafter called as "PMLA Policy") for our whole group (consisting of **Raghunandan Capital (P) Ltd.** having SEBI Regn Nos. in **NSE- INZ000307234**, In **BSE- INZ000307234,** in **MSEI-INZ000307234** for 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.

All concerned are hereby advised to ensure that every possible measure 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 Principal Officer in Equity are as given below:-

Name: **Rahil Uddin**
Designation: Assistant Manager
Contact No: 9958008163
Email: rahil.uddin@rmoneyindia.com

Complete Details of Principal Officer in Commodity are as given below:-

Name: **Saurabh Mittal**
Designation: Director
Contact No: 9897036767
Email: saurabh.mittal@rmoneyindia.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 Directors.

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 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 Director". The details of the designated Director are as given below:-

Complete Details of Designated Director in Equity are as given below:-

Name: **Mr. Rashmi Mittal**
Designation: Director
Contact No: 9639007408
Email: rmcompliance@rmoneyindia.com

Complete Details of Designated Director in Commodity are as given below:-

Name: **Mr. Asha Mittal**
Designation: Director
Contact No: 7599906785
Email: simran.karira@rmoneyindia.com

3. Client Due Diligence Measures (CDD Measures)

1. Client Due Diligence means due diligence carried out on a client referred to in clause (ha) of sub-section (1) of section 2 of the PMLA using reliable and independent sources of identification.

2. The CDD shall have regard to the money laundering and terrorist financing risks and the size of the business and shall include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the registered intermediary or through national risk assessment.

3. The CDD measures comprise the following:
    i. 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 reliable and independent 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;
    ii. Identify the clients, verify their identity using reliable and independent sources of identification, obtain information on the purpose and intended nature of the business relationship, where applicable;
    iii. Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and

verify the identity of that person;

Provided that in case of a Trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

iv. Identifying 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. The beneficial owner shall be determined as under-

a) **where the client is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation: - For the purpose of this sub-clause:-

i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders' agreements or voting agreements;

b) **where the client is a partnership firm**, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation: - For the purpose of this clause:-

"Control" shall include the right to control the management or policy decision;

c) **where the client is an unincorporated association or body of individuals,** the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent.

of the property or capital or profits of such association or body of individuals;

d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e) **Where the client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust, settlor, protector and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

g) **Applicability for foreign investors**: Registered intermediaries dealing with foreign investors' may be guided by 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;

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

v. 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 (iii);

vi. Understand the nature of business, ownership and control structure of the client;

vii. 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.

viii. Registered intermediaries shall 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.

ix. Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

x. Every registered intermediary shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

xi. Where registered intermediary is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND.

4. No transaction or account-based relationship shall be undertaken without following the CDD procedure.

Policy for acceptance of clients

5. All registered intermediaries shall develop client acceptance policies and procedures that aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, they will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients:

i. No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified;

ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined 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. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile;

iii. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC 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; Politically Exposed Persons" (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the PML Rules. The additional norms applicable to PEP as contained in the subsequent paragraph 20 of

the master circular shall also be applied to the accounts of the family members or close relatives / associates of PEPs;

e) Clients in high risk countries. While dealing with clients from or situated 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 suspected, registered intermediaries apart from being guided by the 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 registered intermediaries from entering into legitimate transactions with clients from or situated in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. The intermediary shall specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF;

f) Non face to face clients - Non face to face clients means clients who open accounts without visiting the branches/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients;

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

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

iv. 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.

v. Ensure that an account is not opened where the intermediary is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non - co-operation of the client in providing full and complete information. The registered intermediary shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The registered intermediary shall be cautious to ensure that it does not return securities or money that may be from suspicious trades. However, the registered intermediary shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

i. The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons i.e. the agent-client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

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

iii. The CDD process shall necessarily be revisited when there are suspicions of ML/TF.

Client identification procedure

6. The KYC policy shall clearly spell out the client identification procedure (CIP) 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.

7. Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP**:**

   i. All registered intermediaries shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.

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

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

   iv. 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.

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

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

8. SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time, all registered intermediaries shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

9. Further, the intermediary shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing.

10. Every intermediary shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

    It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to registered intermediaries (brokers, depository participants, AMCs etc.) 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 clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly

implemented by all registered intermediaries and non-compliance shall attract appropriate sanctions.

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

11. Registered intermediaries may rely on a third party for the purpose of -

    i. identification and verification of the identity of a client and

    ii. 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.

12. 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. In terms of Rule 9(2) of PML Rules:

    i. The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;

    ii. The registered intermediary shall take adequate steps to satisfy itself 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;

    iii. The registered intermediary 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;

    iv. The third party is not based in a country or jurisdiction assessed as high risk;

    v. The registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

Risk Management

Risk-based Approach

While accepting and executing a client relationship the Company will adopt a Risk Based Approach as under:

Low Risk	Medium Risk	High Risk
Individual clients, with clean image, not PEP, with investment up to Rs. 50 Lakhs, whose identity and sources of wealth can be easily identified.	Clients over investment of Rs. 50 Lakhs where identity and sources of wealth are not supported by public documents like Income Returns, Registered conveyance Deeds etc.	HNI Clients (having Net worth over 500 Lakhs) with no known sources of Income
Listed Companies	Clients with sudden spurt in volumes or investment without apparent reasons	Clients subsequently becoming suspicious of ML/FT activities
Govt. owned companies, regulated bodies like banks and PMLA regulated intermediaries	Persons in business/ industry or trading activity where scope or history of unlawful trading/business activity dealings is more.	Single Share Companies Or Companies with bearer shares
Day traders and arbitrageurs	Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or Doubtful/dubious.	All Clients of Special Category
Clients having regular relationship or low volumes (e.g. upto 25 lakhs)	Clients having occasional relationship but with moderate volumes (upto 100 lakhs)	Clients having occasional relationship with large volumes (over 100 lakhs)
		Politically Exposed Persons Systems should be there to find out whether a person is PEP- Take reasonable measures to establish source of wealth

		and source of funds on ongoing basis.
		Client accounts opened by professional intermediaries.

The clients shall be shifted from one category to another on real-time basis, if at any time they satisfy the above-mentioned criteria. The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

Review of Policy

To be in compliance with PMLA obligations, the senior management 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. 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; to ensure that the content of these Directives are understood by all staff members; regularly review the policies and procedures on an annual basis on the prevention of ML and TF to ensure their effectiveness and on the basis of documents received from the clients category is modified for High, Medium & Low.

Periodicity of collection of Documents from clients for change in Risk Categorization:

Low Risk	Medium Risk	High Risk
5 Years	2 Years	1 Years

Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures; adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF; undertake client due diligence ("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; have a system in place for identifying, monitoring and reporting suspected ML or TF

transactions to the law enforcement authorities; and develop staff members' awareness and vigilance to guard against ML and TF Clients of Special Category: Special care shall be taken while opening accounts of Clients of Special Category. Such clients include the following

a. Non-resident clients
b. HNI clients (having Net worth over 500 Lakhs)
c. Trust, Charities, NGOs and organizations receiving donations
d. Companies having close family shareholdings or beneficial ownership
e. Politically exposed persons (PEP) of foreign origin
   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)
f. Companies offering foreign exchange offerings
g. 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.
h. Non face to face clients
i. Clients with dubious reputation as per public information available etc.

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

Risk Assessment

13. Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

14. 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.

15. The Stock Exchanges and registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:

    a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
    b. Adoption of a risk based approach to manage and mitigate the risks.

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

Monitoring of Transactions

16. Ongoing monitoring is an essential element of effective KYC procedures. Rmoney can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

17. Rmoney shall have in place a comprehensive transaction monitoring process from a KYC/AML perspective. Rmoney shall put in place strong transaction alerts which will provide proactive signals on suspicious transactions and possible money laundering. The Company has created awareness at each level of department and principal officer along with other officials of the Company shall endeavor to update the list based on current understanding of the market scenario and trading patterns followed by clients. In addition to the alerts from internal sources, the Surveillance & compliance team shall also monitor the alerts provided by the various Exchanges & Depositories.

18. On the basis of criticality of the breach, observation of account behavior, repetitive breaches, the Principal Officer shall send a query to the concerned business. Responses would be expected within 7 working days. If the alerts still persist or the Principal Officer is not satisfied with the responses, then he shall send the query to the Compliance Head for resolution.

19. In case of any account wherein alerts are observed on a regular basis, the risk categorization would be increased based on the consensus of the AML monitoring team and the compliance officer. Such a review would be done at least once every month.

20. Special attention is required for all complex, unusually large transactions / patterns which appear to have no economic purpose. The background including all documents, office records and clarifications pertaining to such transactions and their purpose will be-examine carefully and findings will be recorded. Such findings, records and related documents would be made available to auditors and also to SEBI/Stock Exchanges/FIU-IND/Depositories /other relevant authorities, during audit, inspection or as and when required. These records to be preserved for ten years as required under PMLA 2002

21. It would be ensured that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 or any other notification issued in due course and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority.

Suspicious Transaction Monitoring and Reporting

22. Registered Intermediaries shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

23. 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:

i Clients whose identity verification seems difficult or clients that appear not to cooperate;

ii Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;

iii Clients based in high risk jurisdictions;

iv Substantial increases in business without apparent cause;

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

vi Attempted transfer of investment proceeds to apparently unrelated third parties;

vii Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

24. Any suspicious transaction shall be immediately notified to the **Designated/Principal Officer** within the intermediary. 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 shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall 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 Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

25. 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 registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

26. Paragraph 18 (iii) (f) of this Circular categorizes 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, as 'CSC'. Registered intermediaries are directed that such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting

27. 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.

Record Management

Information to be maintained

28. Registered Intermediaries are required to 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.

Record Keeping

29. Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

30. Registered Intermediaries shall 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 behavior.

31. 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:

    i. the beneficial owner of the account;
    ii. the volume of the funds flowing through the account; and
    iii. 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.

32. Registered Intermediaries 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, 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 thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

33. More specifically, all the registered intermediaries shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

ii. 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.

iii. 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;

iv. 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.

34. Where the registered entity does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

Retention of Records

(a) The Company shall maintain necessary records on transactions, both domestic and international, at least for the minimum period prescribed under the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange / Depositories Bye-laws and Circulars issued from time to time.

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

(c) In situations where the records relate to on-going investigations or transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 for the PML Rules, shall maintain at least for a period of eight years from the date of the transaction or shall be retained until it is confirmed that the case has been closed.

(d) Further, in terms of Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 (herein referred to as D&P Regulations, 2018) notified on October 03, 2018, Rmoney shall preserve the records and documents for a minimum period of eight years.

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

35. The Stock exchanges and the registered intermediaries shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they 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).

36. 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). Corrigendum's dated March 15, 2023 and April 22, 2024 have also been issued in this regard (Annexure 3) and (Annexure 4). The list of Nodal Officers for UAPA is available on the website of MHA.

Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries

37. The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.

38. In terms of Section 12A of the WMD Act, the Central Government is empowered as under:

"(2) For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947

or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

(a) Freeze, seize or attach funds or other financial assets or economic resources—

(i) owned or controlled, wholly or jointly, directly or indirectly, by such person; or

(ii) held by or on behalf of, or at the direction of, such person; or

(iii) derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

(b) prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

39. The stock exchanges and registered intermediaries are directed to comply with the procedure laid down in the said Order.

40. The stock exchanges and registered intermediaries shall:

(i) Maintain the list of individuals/entities ("**Designated List"**) and update it, without delay, in terms of paragraph 2.1 of the Order;

(ii) verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries shall not

Carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), without delay. The details of the CNO are as under:

The Director
FIU-INDIA
Tel. No.: 011-23314458, 011-23314459 (FAX)
Email: dir@fiuindia.gov.in

(iii) Run a check, on the given parameters, at the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc. In case, the clients' particulars match with the particulars of Designated List, stock exchanges and registered intermediaries shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO, without delay;

(iv) Send a copy of the communication, mentioned in paragraphs 59(ii) and 59(iii) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051;

(v) prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall

Under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act;

(vi) File a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs 59(ii) and (iii) above, carried through or attempted through.

41. Upon the receipt of the information above, the CNO would cause a verification to be conducted by the appropriate authorities to ensure that the individuals/entities identified are the ones in the Designated List and the funds, financial assets or economic resources or related services, reported are in respect of the designated individuals/entities. In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under section 12A would be issued by the CNO and be conveyed to the concerned reporting entity so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/entities.

42. Reporting entities shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of Designated Individuals/ Entities

43. The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The registered intermediaries shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

44. All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

45. 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 https://press.un.org/en/content/press- release. The details of the lists are as under:

i. The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: https://www.un.org/securitycouncil/sanctions/1267/press-releases ;

ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

46. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

47. The Stock Exchanges and the registered intermediaries shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

48. The Stock Exchanges and the registered intermediaries shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

49. The Stock exchanges and the registered intermediaries shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions

Carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

50. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

51. The Stock exchanges and the registered intermediaries shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

52. FATF Secretariat after conclusion of each of it's plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the registered intermediaries.

53. The registered intermediaries shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not

Precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

Reporting to Financial Intelligence Unit-India

54. In terms of the PML Rules, registered intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit - India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone: 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in
(For FINnet and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity / Principal Officer Registration related queries)
complaints@fiuindia.gov.in
Website: http://fiuindia.gov.in

55. Registered intermediaries shall carefully go through all the reporting requirements (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Brochures on FIU_p.pdf) and formats that are available on the website of FIU – IND under the Section Home - FINNET 2.0 – User Manuals and Guides -Reporting Format (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Reporting_Format_p.pdf). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU- IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, registered intermediaries shall adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month;

ii. 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 on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules. 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;

iii. The Non-Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month;

iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND;

vi. No NIL reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported;

vii. “Non-profit organization” means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

viii. Every registered intermediary, its Directors, officers and all employees shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential. Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

56. Registered Intermediaries shall not put any restrictions on operations in the accounts where an STR has been made. Registered intermediaries and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

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

    It is further clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

    Confidentiality requirement does not inhibit information sharing among entities in the group.

Designation of officers for ensuring compliance with provisions of PMLA

57. **Appointment of a Principal Officer:** To ensure that the registered intermediaries properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer 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. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary; Provided that such officer shall be an officer at the management level.

58. **Appointment of a Designated Director**: In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

"Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,

b) the managing partner if the reporting entity is a partnership firm,

c) the proprietor if the reporting entity is a proprietorship firm,

d) the managing trustee if the reporting entity is a trust,

e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

f) Such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above".

59. In terms of Section 13 (2) of the PMLA, the Director, FIU – IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

60. Registered intermediaries shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

Hiring and Training of Employees and Investor Education

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

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

63. Investor Education: Implementation of AML/CFT measures requires registered intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for registered intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Registered intermediaries shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT Programme.

Repeal and Savings

64. On and from the issue of this Circular, the circulars listed out in the Appendix to this Circular shall stand rescinded. Notwithstanding such rescission, anything done or any action taken or purported to have been done or taken, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular.

Appendix

The following Circulars shall stand rescinded from the date of issuance of this Circular

1. **SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June 16, 2023 -** Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

2. **SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/0170 dated October 13, 2023 -** Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

3. **SEBI/HO/MIRSD/SEC-5/P/CIR/2023/062 dated April 26, 2023 -** Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries.

4. **SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 –** Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under.

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 Principle Office of the company.

Lists of Red Flag Indicators for Terrorist Financing

Four Lists of Red Flag Indicators for Terrorist Financing

1. Financial and Behavioral 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.

Behavioral 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.

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

Activity Inconsistent with the Customer's Business:

1. 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 non- cooperative countries and territories).
2. The stated occupation of the customer is not commensurate with the type or level of activity.
3. 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).
4. 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.
5. 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.
6. Funds Transfers:
7. 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.
8. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
9. 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.

10. 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.
11. 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.
12. Other Transactions That Appear Unusual or Suspicious:
13. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
14. 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.
15. 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.
16. Banks from higher-risk locations open accounts.
17. Funds are sent or received via international transfers from or to higher-risk locations.
18. Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

3. 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

4. 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 (crowd funding 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.