Giriraj Stock Broking Private Limited

POLICIES & PROCEDURES ADOPTED FOR PREVENTION OF MONEY LAUNDERING
(Issued as per the requirements of PMLA Act 2002)

Master Circular: - Ref. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated- February 03, 2023

Policy created by	**Compliance Team**
Policy reviewed by	**Principal Officer**
Policy reviewed on	**30.09.2025**
Policy Approved by	**Board of Directors**
Policy approved on	**08.10.2025**

Version – 1.5

1. Policy

It is our policy to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

2.1. Written Anti Money Laundering Procedures

We have adopted these written procedures to implement the anti- money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following three specific parameters which are related to the overall 'Client Due Diligence Process':

- ✓ Policy for acceptance of clients
- ✓ Procedure for identifying the clients
- ✓ Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).
- ✓ Risk Management

2.2. Client Due Diligence (CDD)

The CDD measures shall comprise the following:

- ✓ 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 person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

  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.
- ✓ 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, we 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.
- ✓ 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-

Where Client is Individual:

Where the client is an individual, he shall submit to the reporting entity, the Aadhaar number where,

- ✓ he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
- ✓ he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or
- ✓ the proof of possession of Aadhaar number where offline verification can be carried out; or
- ✓ the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid document or the equivalent e-document thereof containing the details of his identity and address; and
- ✓ the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- ✓ such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity

Provided that if the client does not submit the Permanent Account Number, he shall submit one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents including in respect of the nature or business and financial status of the client as may be required by the reporting entity.

[Explanation. - Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by the regulator.]

Where Client is 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: -

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

Where Client is 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;

Where 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.

Where no natural person is identified above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

Where Client is 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

Where 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.

Applicability for Foreign Investors:

For 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.

Provided that where the Regulator is of the view that money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business, the Regulator may permit the reporting entity to complete the verification as soon as reasonably practicable following the establishment of the relationship; and in all other cases, verify identity while carrying out-

- ✓ transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or
- ✓ any international money transfers operations.

<u>As per Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015, Rule 9</u>

- ✓ Every reporting entity shall within [ten days] after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with the Central KYC Records Registry;
- ✓ The Central KYC Records Registry shall process the KYC records received from a reporting entity for de-duplicating and issue a KYC Identifier for each client to the reporting entity, which shall communicate the KYC Identifier in writing to their client;
- ✓ Where a client submits a KYC Identifier to a reporting entity, then such reporting entity shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless -
  - there is a change in the information of the client as existing in the records of Central KYC Records Registry;
  - the current address of the client is required to be verified;
  - the reporting entity considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

- ✓ A reporting entity after obtaining additional or updated information from a client under sub rule (1C), shall as soon as possible furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client.
- ✓ The reporting entity which performed the last KYC verification or sent updated information in respect of a client shall be responsible for verifying the authenticity of the identity or address of the client.
- ✓ A reporting entity shall not use the KYC records of a client obtained from the Central KYC Records Registry for purposes other than verifying the identity or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director;
- ✓ The regulator shall issue guidelines to ensure that the Central KYC records are accessible to the reporting entities in real time.
- ✓ A reporting entity may rely on a third-party subject to the conditions that-
  - the reporting entity immediately obtains necessary information of such client due diligence carried out by the third party;
  - the reporting entity takes 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;
  - the reporting entity is 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;
  - the third party is not based in a country or jurisdiction assessed as high risk;
  - the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

In case of Non-Individuals, additional documents to be obtained from non-individuals, over & above the POI & POA, as mentioned below:

Types of entity	Documentary requirements
Corporate	✓ Copy of the balance sheets for the last 2 financial years (to be submitted every year). ✓ Copy of latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/Whole time director/MD (to be submitted every year). ✓ Photograph, POI, POA, PAN and DIN numbers of whole-time directors/two directors in charge of day to day operations.

	✓ Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly. ✓ Copies of the Memorandum and Articles of Association and certificate of incorporation. ✓ Copy of the Board Resolution for investment in securities market. ✓ Authorised signatories list with specimen signatures.
Partnership firm	✓ Copy of the balance sheets for the last 2 financial years (to be submitted every year). ✓ Certificate of registration (for registered partnership firms only). ✓ Copy of partnership deed. KYC/AML Policy ✓ Authorised signatories list with specimen signatures. Photograph, POI, POA, PAN of Partners.
Trust	✓ Copy of the balance sheets for the last 2 financial years (to be submitted every year). ✓ Certificate of registration (for registered trust only). ✓ Copy of Trust deed. ✓ List of trustees certified by managing trustees/CA. ✓ Photograph, POI, POA, PAN of Trustees.
HUF	✓ PAN of HUF. ✓ Deed of declaration of HUF/ List of coparceners. ✓ Bank pass-book/bank statement in the name of HUF. ✓ Photograph, POI, POA, PAN of Karta.
Unincorporated association or a body of individuals	✓ Proof of Existence/Constitution document. ✓ Resolution of the managing body & Power of Attorney granted to transact business on its behalf. ✓ Authorized signatories list with specimen signatures.
Banks/Institutional Investors	✓ Copy of the constitution/registration or annual report/balance sheet for the last 2 financial years. ✓ Authorized signatories list with specimen signatures.
Foreign Institutional Investors (FII)	✓ Copy of SEBI registration certificate. KYC/AML Policy ✓ Authorized signatories list with specimen signatures.
Army/ Government Bodies	✓ Self-certification on letterhead. ✓ Authorized signatories list with specimen signatures.

Registered Society	✓ Copy of Registration Certificate under Societies Registration Act. ✓ List of Managing Committee members. ✓ Committee resolution for persons authorised to act as authorised signatories with specimen signatures. ✓ True copy of Society Rules and Bye Laws certified by the Chairman/Secretary.

Monitor of compliance

The compliance of the aforementioned provision on identification of beneficial ownership shall be monitored by the Board of Directors.

- ✓ Verifying the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information.
- ✓ Understand the nature of business, ownership and control structure of the client.
- ✓ Conducting 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 our knowledge of the client, its business and risk profile, considering, where necessary, the client's source of funds.
- ✓ We 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; and
- ✓ We 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.
- ✓ We shall register the details of a client, in case of client being a non-profit organisation, 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 we have ended or the account has been closed, whichever is later.
- ✓ Where we are suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, we shall not pursue the CDD process, and shall instead file a STR with FIUIND."
- ✓ No transaction or account-based relationship shall be undertaken without following the CDD procedure."

2.3. Policy for acceptance of clients:

The 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. By establishing such policies and procedures, we 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 will be followed while accepting the clients:

- ✓ No account is opened in a fictitious / benami name or on an anonymous basis or account on behalf of other persons whose identity has not been disclosed or cannot be verified
- ✓ 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.
- ✓ Clients of special category (CSC) - Such clients shall include the following:
  - Non - resident clients
  - High net-worth clients,
  - Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
  - 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 Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. 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."
  - 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 / effectiveness of action against money laundering controls is suspected, 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 centres, 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, we shall apart from being guided by the Financial Action Task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, 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 us 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. We 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.

- Non-face to face clients - Non-face to face clients means clients who open accounts without visiting the branch/offices or meeting the officials of our company. Video based customer identification process is treated as face-to-face onboarding of clients
- Clients with dubious reputation as per public information available etc.
- Clients with foreign exchange offerings.
- The above-mentioned list is only illustrative and we shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

✓ 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.

✓ Ensure that an account is not opened where it is unable to apply appropriate CDD measures/ KYC policies. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to us 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. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. We shall be cautious to ensure that we do not return securities of money that may be from suspicious trades. However, we shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

✓ 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 us, 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.

✓ 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

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

2.4. Client identification procedure:

✓ The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the client relationship, while carrying out transactions for the client or when we have doubts regarding the veracity or the adequacy of previously obtained client identification data. we shall be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

- We shall proactively put in place appropriate risk management systems to determine whether its existing client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the

commercial electronic databases of PEPs. Further, the enhanced CDD measures shall also be applicable where the beneficial owner of a client is a PEP.

- Senior management approval would be obtained 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, we shall obtain approval from Director to continue the business relationship.
- We shall also take reasonable measures 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 using reliable sources including documents / information. We shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by 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 higher authority (Principal Officer).

✓ SEBI has prescribed the minimum requirements relating to KYC from time to time. Considering the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, we shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

✓ Further, we 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 there under so that the we are aware of the clients on whose behalf it is dealing.

✓ We 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 and such other additional requirements that is considered appropriate to enable 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 us 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 us. This shall be strictly implemented by us and non-compliance shall attract appropriate sanctions.

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

✓ We may rely on a third party for the purpose of

- Identification and verification of the identity of a client and

- 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.

✓ 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:

- We shall immediately obtain necessary information of such client due diligence carried out by the third party.
- We 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
- 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;
- The third party is not based in a country or jurisdiction assessed as high risk.
- We shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

2.6. Risk Management

Risk-based Approach:

✓ 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. As such, we shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that we 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.

✓ Further, low risk provisions 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

- In order to achieve this objective, all clients of the branch should be classified in the following category:
  - **High Risk–** Clients who fall under the category of CSC.
  - **Medium Risk** - Customers that are likely to pose a higher than average risk to the broker may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. such as
    - Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.

- Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

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

Risk Assessment:

- ✓ We 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.
- ✓ 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.
- ✓ We 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 we shall ensure:
  - To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
  - Adoption of a risk-based approach to manage and mitigate the risks"
- ✓ The risk assessment shall also consider any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions. These can be accessed at the URL - https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list.

2.7. Monitoring of transactions

- ✓ Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if we understand the normal activity of the client so that it can identify deviations in transactions / activities.
- ✓ We shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. We may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIUIND/ other relevant Authorities, during audit,

inspection or as and when required. These records will be maintained and preserved for a period of five years from the date of transaction between the clients and company.

- ✓ We shall apply client due diligence measures also to existing clients 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.
- ✓ We shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities (Director) within company.
- ✓ Further, the compliance cell of company 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.
- ✓ All regulatory alerts generated by the Market Infrastructure Institutions (MIIs) shall be monitored by the Principal Officer for necessary action to be taken.

2.8. Suspicious Transaction Monitoring and Reporting

- ✓ We 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, we shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.
- ✓ 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:
  - Clients whose identity verification seems difficult or clients that appear not to cooperate
  - Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing/business activity;
  - Clients based in high risk jurisdictions;
  - Substantial increases in business without apparent cause;
  - Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
  - Attempted transfer of investment proceeds to apparently unrelated third parties;
  - 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.
- ✓ Any suspicious transaction shall be immediately notified to the Designated / Principal Officer within organization. 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.

- ✓ 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 we shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.
- ✓ This policy 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'. 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.

Supplemental Guidelines for detecting suspicious transactions under rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 –

- ✓ With a view to revise and update the Red Flag Indicators (hereinafter referred to as 'RFIs'), FIU – IND had constituted a Working Group consisting of members from various stakeholders in the securities market, FIU-IND and SEBI. Based on the recommendation of the Working Group, certain RFIs have been identified. It has been felt that these RFIs should be implemented by the Reporting Entity (Res) concerned for generation of alerts and identification of suspicious transactions.
- ✓ Sub – Rule (3) of Rule 7 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended, empowers Director, FIU-IND to issue guidelines in consultation with Regulator for detecting suspicious transactions. These guidelines are being issued under the said Rule.
- ✓ These RFIs which are proposed to be implemented are mentioned in Annexure – A. Further, it is pertinent to mention that these RFIs are in addition to the RFIs issued vide FIU-IND's communication dated 11th March, 2016 issued vide F. No. 9-6/AG-11/2012/FIU-IND.
- ✓ The alerts generated by using the indicators as given in the guidelines should be properly analysed with a view to identify suspicious transactions as defined under the PMLA Rules, and if we conclude that case appears to be a suspicious transaction, then the case may be brought to the notice of FIU-IND by filling Suspicious Transaction Reports (STRs) following the prescribed procedure in this regard.
- ✓ The thresholds prescribed in these alert indicators are indicative and are derived based on data analysis and back – testing carried out by the Working Group. We are free to adopt stricter criteria and lower thresholds, but we may not adopt criteria less strict than that which is provided by FIU – IND herein in order to mitigate eminent AML / CFT risks specifically in cases where purposeful avoidance of such thresholds is observed by the organization
- ✓ It should be noted that the analysis process within the AML / CFT organizational setup within the company should be carried out in a manner that it should not lead to tipping-off. In this regard, we are cautioned that the requirement of confidentiality regarding reporting of transactions to FIU – IND extends not only to the customers concerned but also to other care must be taken to ensure that the fact of whether an STR has been filed in relation to a specific transaction or alert is not directly or indirectly disclosed. Any deviation in this regard will be viewed strictly.

- ✓ Designated Director and Principal Officer of the company concerned to implement the guidelines with immediate effect with reference to Financial Intelligence Unit-India (FIU-IND) letter ref. no. F. No. 9-2/2021/Intermediaries/FIU-IND dated July 21, 2022
- ✓ Further, penalties for non – compliance with obligation under Chapter IV of PMLA (including obligations to report STRs and to have in place an effective mechanism to detect and report STRs) may range up to Rs. 1 lakh per non – compliance.

Annexure A – Indicative Alert Indicators

Serial No	Alert Source	Alert Indicator	Indicative Rule / Scenario
1	Transaction Monitoring	TM 11 – Fund Received from Non – Clients	Single or multiple transfer of funds more than 1 Cr in a calendar month in brokers accounts which are not reported as clients.
2	Transaction Monitoring	TM 12 – Margin Trading	Sudden increase in the funding amount of Margin Trading Facility (MTF) exposure. 1. By more than 50% of MTF exposure of previous month AND; 2. With a value of more than Rs. 10 crores.
3	Transaction Monitoring	TM 13 – Off Market Transfer to unrelated accounts	1. Only for Reason code/s - off – market sale – Gift - Donation And; 2. Valuation per debit transaction will be > 25 lacs AND; 3. Exclude accounts with same PAN, mobile, email id, same bank details (IFSC + ac no) (same mobile / email / bank details in multiple demat account will be treated as related accounts) and family flag is enabled AND; 4. Valuation is > 5 times of income range.
4	Transaction Monitoring	TM 13A – Suspicious Off Market Credit and Debit	1. Customer receive credit / demat of 50,000 shares or shares worth Rs. 25 lakhs and above by single transaction or series of transactions in an ISIN AND; 2. 80% or more of credited shares gets debited by way Off Market transfers to 3 or more than 3 unrelated accounts AND; 3. Only Listed Equity Shares will be considered for this alert. (Monthly Frequency) Short Span of time is within 30 days.
5	Transaction Monitoring	TM 13B – Off Market Delivery in Unlisted Scrip	1. Single or Series of Transactions where more than 5,00,000 unlisted equity shares have been transferred within period of 1 month AND; 2. Off – Market Transfers with Reason Code "Off – Market Sale", "Donation" and "Gift" will be considered AND;

			3. Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer to own accounts. (Monthly Frequency)
6	Transaction Monitoring	TM 13C – Gift, Donation related off-market transfer	1. Transaction value of such transaction is beyond 5 times of income range / Net worth 9as updated in demat account) on higher side as provided by the BO AND; 2. Listed Equity Shares will be considered AND; 3. Debit transaction specific reason codes > 5 lacs in value AND; 4. For Reason code/s - Family Account Transfer - Gift - Donation
7	Transaction Monitoring	TM 13D – Off Market Transfer at variance with market value	1. Off market transfers with reason code "Off – Market Sale" AND; 2. Difference of +/- 50% difference in consideration value mentioned by BO and prevailing market value of Equity Shares AND; 3. Only Listed Equity Shares will be considered AND; 4. Minimum transaction value for alert will be Rs. 25 lakhs
8	Transaction Monitoring	TM 13E – Off Market transfer in suspicious scrip	1. Off Market single or series of transactions having value of Rs. 2 lakh and above AND; 2. Suspicious Scrips for which unsolicited SMSs were circulated will be taken from below URLs BSE: https://www.bseindia.com/attention_investors.aspx NSE: https://www.nseindia.com/regulations/unsolicited-messages-report
9	Employee initiated	EI 13 – Suspicious Closure of Account	1. Accounts closed within 30 days of opening of Account and single or series of debit transactions (On Market, Off Market including IDT Transfer) with value > 10 lacs AND; 2. Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer to own accounts. Also, if securities received in source account through transmission, then the same will be excluded.

2.9. Record Management

Information to be maintained

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

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

Record Keeping

- ✓ We shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.
- ✓ We 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 behaviour.
- ✓ Should there be 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, we shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:
  - the beneficial owner of the account;
  - the volume of the funds flowing through the account; and
  - for selected transactions:
    - the origin of the funds
    - the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
    - the identity of the person undertaking the transaction;
    - the destination of the funds;
    - 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 there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.
- ✓ Maintenance of the records of the identity of clients. –
  - Every reporting entity shall maintain the physical copy of records of the identity of its clients obtained, after filing the electronic copy of such records with the Central KYC Records Registry.

- The records of the identity of clients shall be maintained by a reporting entity in the manner as may be specified by the Regulator from time to time.
- Where the reporting entity does not have records of the identity of its existing clients, it shall obtain the records within the period specified by the regulator, failing which the reporting entity shall close the account of the clients after giving due notice to the client.
    - Explanation. - For the purpose of this rule, the expression "records of the identity of clients" shall include updated records of the identification data, account files and business correspondence.

✓ Furnishing of Report to Director. –

- The persons shall furnish reports on the measures taken to the Director every month by the 10th day of the succeeding month.
- The Director may relax the time interval above to every three months on specific request made by the reporting entity based on reasonable cause.

✓ Expenses for audit. –

- The expenses of, and incidental to, audit referred to in sub-section (1A) of section 13 of the Act (including the remuneration of the accountant, qualified assistants, semi-qualified and other assistants who may be engaged by such accountant) shall be paid in accordance with the amount specified in sub-rule (2) of rule 14B of the Income-tax Rules, 1962 for every hour of the period as specified by the Director.
- The period referred to in sub-rule (1) shall be specified in terms of the number of hours required for completing the report.
- The accountant referred to in sub-section (1A) of section 13 of the Act shall maintain a time sheet and submit it to the Director, along with the bill.
- The Director shall ensure that the number of hours claimed for billing purposes is commensurate with the size and quality of the report submitted by the accountant.

✓ More specifically, we 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:

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

- Where we do 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 Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

Retention of Records

- ✓ We shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and company.
- ✓ We are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between the clients and company has ended or the account has been closed, whichever is later.
- ✓ In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.
- ✓ Records of information related to transactions, whether attempted or executed, which are reported to the Director, Financial Intelligence Unit – India (FIU – IND), as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and company.

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

- ✓ 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).
- ✓ 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 for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021. Corrigendum's dated March 15, 2023 and April 22, 2024 have also been issued in this regard. The list of Nodal Officers for UAPA is available on the website of MHA.
- ✓ Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The Government is also empowered to

prevent the entry into or transit through India of Individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

- ✓ We shall ensure effective and expeditious implementation of the procedure laid down in the UAPA Order dated February 02, 2021 as listed below:
  - On receipt of the updated list of individual's/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities) from the Ministry of External Affairs (MHA)' and forwarded by SEBI, we shall take the followings steps:
    - 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.
    - 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:
      - 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://main.un.org/securitycouncil/en/sanctions/1267.
      - The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea https://main.un.org/securitycouncil/en/sanctions/1533.
    - We are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. We 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.
    - We will maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with them.
    - We shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.
    - In case, particulars of any of customers match with the particulars of designated individuals/entities, we shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed through e-mail at jsctcr-mha@gov.in.
    - We shall also send the copy of the communication mentioned above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla

Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.

- In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, we shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA, at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed through e-mail at jsctcr-mha@gov.in.
- We shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts carried through or attempted, as per the prescribed format.
- 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 company.
- We shall consider 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.

✓ On receipt of the particulars, Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by us are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by us are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

✓ In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned depository under intimation to SEBI and FIU-IND so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for benefit of the designated individuals / entities or any other person engaged in or suspected to be engaged in terrorism. The order shall take place without prior notice to the designated individuals/entities.

✓ Implementation of requests received from foreign countries under U.N. Securities Council Resolution 1373 of 2001.

- U.N. Security Council Resolution 1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and

entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

- To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] nodal officer for the UAPA for freezing of funds or other assets.
- The Central [designated] nodal officer for the UAPA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officer in SEBI and FIU-IND. The proposed designee, as mentioned above would be treated as designated individuals/entities.
- Upon receipt of the requests by these Nodal Officers from the Central [designated] nodal officer for the UAPA, the list would be forwarded to us and the procedure shall be followed.
- The freezing orders shall take place without prior notice to the designated persons involved.

✓ Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

- Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to us.
- We shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Central [designated] nodal officer for the UAPA as per the contact details given above within two working days.
- The Central [designated] nodal officer for the UAPA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and company. However, if it is not possible for any reason to pass an order unfreezing the assets within five working days, the Central [designated] nodal officer for the UAPA shall inform the applicant expeditiously.

✓ Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

- All Orders under section 51A of the UAPA relating to funds, financial assets or economic resources or related services, would be communicated to stock exchanges, depositories and company through SEBI.

✓ Prevention of entry into or transit through India:

- As regards prevention of entry into or transit through India of the designated individuals, the UAPA Nodal Officer in the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry or the transit through India. The order shall take place prior notice to the designated individuals / entities.
- The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in the Foreigners Division of MHA.

2.11. Procedure for implementation of Section 12A of the "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005:

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as the Act'] reads as under -

- ✓ No person shall finance any activity which is prohibited under this 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.
- ✓ For prevention of financing by any person of any activity which is prohibited under this 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-
  - freeze, seize or attach funds or other financial assets or economic resources-
    - owned or controlled, wholly or jointly, directly or indirectly, by such person, or
    - held by or on behalf of, or at the direction of, such person, or
    - derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

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 this 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 may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."
- ✓ We shall maintain the list of individuals/entities ("Designated List") and update it, without delay.
- ✓ We shall 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, we 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

- ✓ We shall 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, we 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.
- ✓ We shall send a copy of the communication, mentioned in 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.
- ✓ We shall 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;
- ✓ We shall file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered above, carried through or attempted through.

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.

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

2.12. List of Designated Individuals/ Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at https://press.un.org/en/content/press-release. The details of the lists are as under:

- 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.
- 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.

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

Full details of accounts bearing resemblance with any of the individuals/entities in the list 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.70.

We 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

2.13. Jurisdictions that do not or insufficiently apply the FATF Recommendations

- ✓ 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.
- ✓ We will consider the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. Further we are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

2.14. Reporting to Financial Intelligence Unit-India

- ✓ In terms of the PML Rules, we 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

- ✓ We 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, we shall adhere to the following:

- The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall 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 3of 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.
- The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;
- Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.
- No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.
- Non-profit organization" means any entity or organisation, 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).
- We, our 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.

- ✓ We shall not put any restrictions on operations in the accounts where an STR has been made. Company and its 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 we, 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 we 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.

2.15. Designation of officers for ensuring compliance with provisions of PMLA

- ✓ **Appointment of a Principal Officer:** To ensure that we properly discharges its 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.

Mr. Vinay Jajodia was appointed as Principal Officer and the same was intimated to the FIU-IND.

Names, designation and addresses (including email addresses) in case of change in 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU. 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.

- ✓ **Appointment of a Designated Director:** In addition to the existing requirement of designation of a Principal Officer, we 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

- the Managing Director or a Whole-Time Director duly authorizes by the Board of Directors if the reporting entity is a company,
- the managing partner if the reporting entity is a partnership firm,
- the proprietor if the reporting entity is a proprietorship firm,
- the managing trustee if the reporting entity is a trust,
- 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

- 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."

Mr. Kuntal Laha was appointed as Designated Director of company and the same has been intimated to the FIU-IND.

- ✓ 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 company to comply with any of its AML/CFT obligations.
- ✓ We shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

FIU-IND vide its communication dated May 23, 2022, has informed about the fresh registration of the Reporting Entities (REs) in FIN net 2.0 system from 19.01.2022.

As part of the envisaged, FIN net 2.0 system we are registered in FIN net 1.0 is required to re-register in FIN net 2.0 module. Further, it may be noted that as part of the re-registration exercise we have register Principal Officer as well as Designated Director also in FIN net 2.0 module

2.16. Employees' Hiring/Employee's Training/ Investor Education

- ✓ **Hiring of Employees**

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

- ✓ **Employees' Training**

  We will 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.

- ✓ **Investors Education**

  Implementation of AML/CFT measures requires us 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 us to sensitize its clients about these requirements as the ones emanating from AML and CFT framework. We shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

2.17. Review of Policy

This Policy will be reviewed on periodic basis by the Compliance Officer and Principal officer and if there are any changes made to the policy, the same shall be placed before the Board at its first meeting held after such changes are introduced and the same is made available on our website. For its effectiveness since the person reviewing the policy should be different from the person framing the policy.

2.18. Re-KYC of Clients

- ✓ We need to periodically update customer identification documents in their records of account holders to adhere to the KYC norms issued by the extant Market Regulator(s), Stock Exchange(s), Depositories and other Agencies. Re-KYC is the process of a business for re-identifying and verifying the identity of its existing clients.
- ✓ The objective of the Re-KYC is to identity theft, Prevention of Terrorist Financing, Money Laundering and Financial Fraud. KYC allows to understand the Customer better and manage risks prudently. Re-KYC is mandatory and there is no escaping the paperwork while investing in financial products.
- ✓ Personal information needs to be provided and has to be signed by the account holder of company. The KYC Team is mandated to periodically update its Client's identification data including the Client's photograph, a proof of identity, an NRI status proof and a proof of address. The KYC updation of the Clients shall be done once in every 2 years even if there is no change in the identity or address of the Client.

2.19. Other Principles

We shall ensure the following:

- ✓ We shall ensure that the content of these Directives is understood by all staff members
- ✓ We will regularly review the policies and procedures on the prevention of ML and TF on an annual basis 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
- ✓ We will adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF
- ✓ We will 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
- ✓ We have in system a place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
- ✓ We will develop staff members' awareness and vigilance to guard against ML and TF.
- ✓ Role of Internal Audit and Compliance Function to ensure compliance with the Policies
- ✓ The Internal Audit function and compliance function should work in coordination to identify the non-compliance with the Provisions of PMLA and ensure compliance

[Annexure 1]

SEBI Directives on Online KYC Process

SEBI vide Circular no. SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 informed regarding Clarification on Know Your Client (KYC) Process and Use of Technology for KYC.

SEBI held discussions with various market participants and based on their feedback and with a view to allow ease of doing business in the securities market, it has been decided to make use of following technological innovations which can facilitate online KYC. In order to enable the Online KYC, Client's KYC can be completed through online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under e-Sign, in the following manner:

- ✓ The client visits the website/App/digital platform of company and fills up the online KYC form and submits requisite documents online.
- ✓ The name, photograph, address, mobile number, email ID, Bank details of the client shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under e-Sign and the same shall be verified as under:
  - Mobile and email is verified through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of client accepted as part of KYC should preferably be the one seeded with Aadhaar. (we shall ensure to meet the requirements of the mobile number and email as detailed under SEBI circular no. CIR/MIRSD/15/2011 dated August 02,2011)
  - Aadhaar is verified through UIDAIs authentication / verification mechanism. Further, in terms of PML Rule 9 (16), we shall, where the client submits his Aadhaar number, ensure that such client to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15). We shall not store/ save the Aadhaar number of clients in their system. e-KYC through Aadhaar Authentication service of UIDAI or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from the date of carrying out KYC. In terms of SEBI circular No. CIR/MIRSD/29/2016 dated January 22, 2016 the usage of Aadhaar is optional and purely on a voluntary basis by the client.
  - 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. (Explanation: based on bank details in the copy of the cancelled cheque provided by the client, the money is deposited into the bank account of the client to fetch the bank account details and name.) The name and bank details as obtained shall be verified with the information provided by client.
  - Any OVD other than Aadhaar shall be submitted through Digi Locker / under eSign mechanism.
- ✓ In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) "Officially Valid Documents" means the following:
  - the passport,

- the driving licence,
- proof of possession of Aadhaar number,
- the Voter's Identity Card issued by Election Commission of India,
- job card issued by NREGA duly signed by an officer of the State Government and
- the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator.

✓ Further, Rule 9(18) of PML Rules states that in case OVD furnished by the client does not contain updated address, the document as prescribed therein in the above stated Rule shall be deemed to be the OVD for the limited purpose of proof of address.

✓ PML Rules allows a client to submit other OVD instead of PAN, however, in terms of SEBI circular No. MRD/DoP/Cir- 05/2007 dated April 27, 2007 the requirement of mandatory submission of PAN by the client for transaction in the securities market shall continue to apply.

✓ Once all the information as required as per the online KYC form is filled up by the client, KYC process could be completed as under

- The client would take a print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to us under eSign, or
- Affix online the cropped signature on the filled KYC form and submit the same to the company under eSign.

✓ We shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the client in cases where the client has given address other than as given in the OVD. In such cases of return of the intimation letter for wrong / incorrect address, addressee not available etc, no transactions shall be allowed in such account and intimation shall also sent to the Stock Exchange and Depository.

✓ 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 client 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.

✓ SEBI vide circular no. MIRSD/Cir- 26 /2011 dated December 23, 2011 had harmonized the IPV requirements for the intermediaries. In order to ease the IPV process for KYC, the said SEBI circular pertaining to IPV stands modified as under:

- IPV/ VIPV would not be required when the KYC of the client is completed using the Aadhaar authentication / verification of UIDAI.
- IPV / VIPV shall not be required by us when the KYC form has been submitted online, documents have been provided through Digi Locker or any other source which could be verified online.

Features for online KYC App –

We may implement their own Application (App) for undertaking online KYC of client. The App shall facilitate taking photograph, scanning, acceptance of OVD through Digi locker, video capturing in live environment, usage of the App only by authorized person of the company. The App shall also have features of random action initiation for client

response to establish that the interactions not pre-recorded, time stamping, geo-location tagging to ensure physical location in India etc. is also implemented. We shall ensure that the process is a seamless, real-time, and secured, end-to-end encrypted audio-visual interaction with the client and the quality of the communication is adequate to allow identification of the client beyond doubt. We shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. We shall before be rolling out and periodically, carry out software and security audit and validation of their App. We may have additional safety and security features other than as prescribed above.

Feature for Video in Person Verification (VIPV) for Individuals –

To enable ease of completing IPV of a client, we may undertake the VIPV of an individual client through their App. The following process shall be adopted in this regard:

- ✓ We through their authorized official, specifically trained for this purpose, may undertake live VIPV of an individual client, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.
- ✓ The VIPV shall be in a live environment.
- ✓ The VIPV shall be clear and still, the client in the video shall be easily recognizable and shall not be covering their face in any manner.
- ✓ The VIPV process shall include random question and response from the client including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.
- ✓ We shall ensure that photograph of the client downloaded through the Aadhaar authentication / verification process matches with the client in the VIPV.
- ✓ The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.
- ✓ We may have additional safety and security features other than as prescribed above.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff/Employees/and Directors of the Company.

For M/s. Giriraj Stock Broking Private Limited,