MEHTA

REWARDING RELATIONSHIPS

MEHTA EQUITIES LIMITED

ANTI MONEY LAUNDERING POLICY

Background-

The PMLA came into effect from 1st July 2005. Necessary Notifications /Rules under the said Act were published in the Gazette of India on 1st July, 2005 by the Department of Revenue, Ministry of Finance, and Government of India. Further, SEBI had issued the Guidelines on Anti Money Laundering Standards vide their notification No. ISD/CIR/RR/AML/1/06 dated 18 January 2006 and had issued the obligations on the intermediaries registered under Section 12 of SEBI Act, 1992 to adopt a written AML policy framework and to implement it in true spirit. The PMLA has been further amended vide notification dated March 6, 2009 and inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) will now be treated as a scheduled offence under schedule B of the PMLA.

Subsequently SEBI has issued the master circular on AML/CFT on December 31, 2010, July 04, 2018, Oct 15, 2019; June 16, 2023 and October 13, 2023, June 06, 2024 and explained a detailed account of the procedures and obligations to be followed by all registered intermediaries to ensure compliance with AML/CFT directives.

Definition & Applicability-

Money laundering can be defined as cleaning of dirty money obtained from any/ all sources or activities (legitimate or illegitimate) including drug trafficking, organized & unorganized crime, fraud, terrorism etc with the objective of hiding its source & rendering it in legally usable form. It is an act or attempted act to conceal or disguise the identity of illegally obtained proceeds, so that they appear to have originated from legitimate sources. The process of money laundering (which went through placement, layering and integration in normal circumstances) involves creating a web of financial transactions so as to hide the origin of or the true nature of these funds.

The circular shall also apply to all the Branches and Authorized persons located abroad if any especially in countries that do not or insufficiently apply the FATF Recommendations, to the extent local laws and regulations permit. When local applicable laws and regulations prohibit implementation of these requirements, the same shall be brought to the notice of SEBI. In case there is a variance in CDD/AML standards prescribed by SEBI and the regulators of the host country, branches/overseas subsidiaries of intermediaries are required to adopt the more stringent requirements of the two.

Regulatory supervisions-

The GOI has set up an independent body/agency namely financial intelligence unit (FIU India) on November 18, 2004 to counter the menace of money laundering, which will report directly to Economic Intelligence Council headed by Finance Minister.
FIU India has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information related to suspected financial transactions. The agency is also responsible for coordination with the national & international intelligence & enforcement agencies including FATF, formulation and implementation of policies, acting against the culprit within the national boundary or regulatory stretch to pursue the global effort against money laundering, terror financing and related crimes.

Objective

The objective of the policy is to control the menace of money laundering by investigating all integrated or non-integrated financial / securities transactions, increasing due diligence of suspicious entities or high risk clients, maintaining a strict policy, practices & procedure to reduce the risk of ML/TF and reporting to all the regulatory bodies including FIU. The Company shall –

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

.

The policy's objective is to manage the risk created by all deceptive/ illicit/illegal/fraudulent /unfair/ unethical activities or practices prevailing or supposed to prevail within the organization or exists during its operations.

Details of Designated Director	**Details of Principal Officer**
Name- Prashant Bhansali	Name- Ghanshyam Dadhich
Contact No: 022-61507100	Contact No: 022-61507100
E-mail- compliance@mehtagroup.in	E-mail-compliance@mehtagroup.in

Implementation of the policy-

The act, rules, regulations, notifications, guidelines and circular issued by SEBI or other regulatory bodies has imposed an obligation on Intermediaries to form a legal framework.
In additional to different measures, the legal framework must include identity of client, maintenance of records & furnishing information to FIU India. The policy shall stress more on customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis.

The principal officer will act as a single reference point for all the money laundering related measures and shall be responsible for all the policies modification, alteration and implementation. The principal officer will play an active role in monitoring, identification, assessment and reporting of all potentially suspicious transaction.

Customer Verification and Acceptance Policy

The Company shall establish and implement a robust Customer Verification and Acceptance Policy to ensure that no account is opened or maintained in the name of any person or entity with a known criminal background, or appearing in any sanctions, debarred, or restricted lists issued by competent authorities in India or abroad.

Prior to accepting any new client, the Company shall verify whether the client's identity appears in any of the following lists or categories:

- United Nations Security Council (UNSC) Sanctions Lists;
- SEBI Debarred Entities / Persons;
- Financial Action Task Force (FATF) high-risk or non-cooperative jurisdictions;
- Any person or entity subject to criminal or civil proceedings, or banned by any enforcement or regulatory agency globally.

The KYC/Surveillance Team shall continuously monitor and scan all existing and prospective client accounts to ensure that no relationship is established or maintained with any individual or entity appearing in the above-mentioned lists. Any resemblance or positive match identified shall be immediately reported to the Compliance Officer and Principal Officer for necessary regulatory action.

In-Person Verification (IPV)

The Company shall conduct compulsory In-Person Verification (IPV) of every client as part of the account opening process, in accordance with SEBI and Exchange guidelines.

- **Offline Mode:**
  Clients shall be verified by one or more authorized representatives or connecting entities of the Company (such as employees or authorised persons). In remote areas or where personal meetings are not feasible, IPV may be carried out through webcam or live video interaction.

- **Online Mode:**
  For online account openings, IPV shall be performed through a live selfie verification process on the Company's web portal in compliance with regulatory norms.

No account shall be opened in anonymous, fictitious, or benami names under any circumstances. Before onboarding, necessary background checks shall be conducted using publicly available information and regulatory sources to confirm that the client is not associated with any adverse regulatory, criminal, or enforcement action.

All verification activities, records, and results shall be documented, preserved, and periodically reviewed by the Compliance Department to ensure continuous adherence to the Prevention of Money Laundering Act (PMLA), 2002, and related regulatory guidelines.

Fully KYC-Compliant Clients:

Only those clients who fulfil at least the minimum KYC requirements applicable to their respective category shall be accepted under the normal category. Clients identified as suspicious, dubious, or high-risk must comply with additional due diligence requirements as prescribed by the KYC/Compliance Department.

All mandatory fields in the KYC forms must be duly completed, and the supporting documents must be verified against originals, either physically or through webcam verification, DigiLocker, Income Tax website, UIDAI, or any other reliable verification source.

Customer Continuation Policy

The Company shall permit continuation of business relationships with clients only in the form and manner consistent with the documents and declarations submitted at the time of account opening.

Any material change in the client's composition, type, constitution, control, shareholding pattern, or financial status shall be immediately communicated to the Company by the client.

The Company shall ensure that financial details of clients are reviewed and updated annually or periodically as stipulated by SEBI, to ascertain the financial soundness and risk profile of each client.

Failure to disclose or update material changes in a timely manner may result in restriction, suspension, or termination of the client relationship, as deemed appropriate by the Compliance Department.

Clients of Special category or politically exposed persons-

All special category clients shall be accepted with due care and documents/ records should be scrutinized minutely in almost all aspects. Clients with dubious reputation as per public information available etc. Such Other persons who as per our independent judgment may be classified as Client of Special Category (CSC).

In case we have reasons to believe that any of our existing / potential customer is a politically exposed person (PEP) we must exercise due diligence, to ascertain whether the customer is a

politically exposed person (PEP), which would include seeking additional information from clients and accessing publicly available information etc.

The dealing staff must obtain senior management`s prior approval for establishing business relationships with Politically Exposed Persons. In case an existing customer is subsequently found to be, or subsequently becomes a PEP, dealing staff must obtain senior management`s approval to continue the business relationship. We take reasonable measures to verify source of funds of clients identified as PEP.

The client are being identified by using reliable sources including documents / information and obtained adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship. The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the Guidelines.

Each original document should be seen prior to acceptance of a copy. Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority.

While accepting a client the underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

Customer Identification policy-

Establish identity & address of client and other details with sufficient proof - No account shall be opened or continued where MEL is unable to complete new due diligence measure with respect to verifiable documents from time to time (with respect to even change in composition/status/ type/control etc).
All the documents shall be accepted as stated/specified by SEBI and/or Exchanges. Obtain complete & sufficient information about the client to identify the actual beneficiary of the account or on whose behalf, transaction has been carried out (i.e. the entity/person behind the transaction). The account should be investigated to find out, who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It shall also incorporate those persons who exercise ultimate effective control over a legal person or arrangement.

Verify the client's / customer's identity using the reliable & independent source/data/ documents/information.

Conduct on-going due-diligence of the entire clients and increased due diligence for high-risk category clients. Scrutinise the account/client to ensure that transactions are in line with the client's background, financial strength, risk profiling, its activities and pattern. Third party reliance for Customer Due Diligence (CDD) is subject to conditions specified in rule 9(2) of PML Act and shall be in accordance with SEBI guidelines.

Identification of Beneficial Ownership

a) For clients other than individuals or trusts:

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

The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest. *SEBI master circular no SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091date June 16, 2023 & SEBI circular no.* SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/*0170 dated October 13, 2023 has amended* Explanation: Controlling ownership interest means ownership of/entitlement to:

- more than **10**% of shares or capital or profits of the juridical person, where the juridical person is a company;
- more than **10**% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- more than **15**% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

In cases where there is doubt under the clause above as to whether the person with a controlling ownership interest is the beneficial owner, or where no natural person exercises control through ownership interests, the beneficial owner shall be the natural person who exercises control over the juridical person through voting rights, agreements, arrangements, or any other means.

b) For client which is a trust:

Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with **10**% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership. MEL shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

c) Exemption in case of listed companies:

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

d) Applicability for foreign investors:

Members dealing with foreign investors‟ viz., Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued vide SEBI circular

SEBI/HO/AFD-2/CIR/P/2022/175 Dated December 19, 2022 and amendments thereon for the purpose of identification of beneficial ownership of the client.

Further in case where no natural person is identified under clauses 1 (a) or 1 (b) above, the identity of the relevant natural person who holds the position of senior managing official should be obtained and keep n record.

We shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half-yearly internal audits and report to Board of Directors on half-yearly basis.

We verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is conducted, corroborating the information provided in relation to paragraph (c).

i. Understand the ownership and control structure of the client.
ii. Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and
iii. MEL 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 doubt the adequacy or veracity of previously obtained client identification data, and
iv. Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process. such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients.
v. No transaction or account-based relationship shall be undertaken without following the CDD procedure.
vi. Every registered intermediary 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 the registered intermediary has ended or the account has been closed, whichever is later
vii. Where registered intermediary is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND."

Client's Reluctance to Provide Documents or Originals:
If a client exhibits reluctance to produce original documents or fails to provide additional information or documentation when requested, the KYC/Compliance Department shall assess the situation carefully. The account may be opened only after due verification and satisfactory justification of such reluctance.

However, where there is sufficient reason to believe that the client is high-risk, non-cooperative, or unwilling to comply with the KYC requirements, the account shall not be opened.

Any failure by a prospective client to provide satisfactory evidence of identity must be documented and reported to the higher authority within the intermediary for appropriate action.

Risk Management

Risk Based Approach: Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' ownership structure, 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. These parameters should enable classification of clients into low, medium and high risk. Clients of special category may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile on best effort basis. In line with the risk- based approach, type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

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. 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. The assessment where applicable may be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required

Risk profiling of the clients

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.
The aim of risk profiling to differentiate different level of due diligence and monitoring of clients in relation to Risk level associated with it.

The factor of risk perception will depend on client's location, nature of business activities, turnover, nature of transaction, manner & mode of payment, amount associated, nature of securities hold/traded, mode of transaction, trading pattern, ownership pattern etc.

Category of clients-

A-High Risk, B- Medium Risk, C- Low risk

For the purpose of effective implementation of KYC policy and AML Standards, Compliance Officer monitors transactions of all customer accounts on concurrent basis, on the basis of AML Alerts raised by back office system as well as Alert files provided by Exchanges and CDSL. MEL has put in place a system of periodical review of as per risk categorization of accounts.

Risk Profiling of Clients is done as per Client Category, in order to differentiate different level of due diligence and monitoring of clients in relation to Risk level associated with it.
Periodicity for Re confirmation of KYC as per Risk Profiling of Client is as follows:

A. High Risk Categorized Client due diligence or Rekyc to be carried out at least once in a year.

B. Medium Risk Categorized Client Due diligence or Re Kyc confirmation to be carried out atleast once in a 3 years or as when due diligence of Client is required.

C. Low risk Category Clients Due diligence or Re Kyc confirmation to be carried out at least once in a 5 years or as when due diligence of Client is required.

Classifications of Client Accounts on basis of Categorization are as follows:

High Risk Clients:

The following categories of clients shall be classified as High Risk at the time of onboarding, in line with the Prevention of Money Laundering Act, 2002 (PMLA), SEBI AML–CFT guidelines, and Financial Action Task Force (FATF) recommendations:

a. Clients of Special Category

Clients belonging to special categories, including but not limited to:

- Non-Resident Indians (NRIs)
- Trusts, charities, non-governmental organizations (NGOs), and organizations receiving donations
- Companies having complex ownership structures, including complex family shareholding or opaque beneficial ownership arrangements

b. Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) of foreign origin, as defined under clause (db) of sub-rule (1) of Rule 2 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, shall be categorized as High Risk.

The additional due diligence measures applicable to PEPs, as prescribed under paragraph 14 of the SEBI Master Circular, shall also apply to:

- Family members of PEPs
- Close relatives and associates of PEPs
- Politically Exposed Persons (PEPs) of India

c. FATF-related High-Risk Clients / Jurisdictions

Clients resident in, incorporated in, or having significant business relationships with jurisdictions identified by FATF as:

- High-Risk Jurisdictions subject to a Call for Action, or

- Jurisdictions under Increased Monitoring

- Clients transacting through or receiving funds from shell banks, or entities located in FATF-identified high-risk or non-cooperative jurisdictions.

d. Non Face-to-Face and Other High-Risk Clients

- Non face-to-face clients, i.e., clients who have opened accounts without visiting the office/branch or meeting officials in person. (Video-based Customer Identification Process (V-CIP) shall be treated as face-to-face onboarding.)

- Clients with dubious reputation, adverse media coverage, or negative public information available from reliable sources.

Post-registration due diligence shall be conducted on a regular basis, taking into account the transactions executed by such clients. Based on the review, if the client's transactions are found to be satisfactory, the risk category may be downgraded to Medium Risk. However, if any suspicious activity is observed based on the client-provided information or transaction patterns, the risk category may be retained as High Risk, subject to approval by the Internal Compliance Committee or the Compliance Officer, as applicable.

Medium Risk Category Clients

In cases where the:

i. Client's reluctance to provide documents or showing it in original.
ii. Third party reliance for Customer Due Diligence (CDD)
iii. Client's identity is matching with any person having known criminal background or client inclusion in any of the list, which include UN /SEBI Debarred entities/ FATF, etc. or is banned in any other manner of criminal or civil proceedings of any enforcement / regulatory agency worldwide.
iv. Companies wherein the shareholding structure is complex/ having close family shareholding or beneficial ownership.
v. Partnership firms and Limited Liability Partnership Firms
vi. HUF

Post-registration due diligence shall be conducted based on the transactions executed by such clients within a specified timeframe. If the transactions are found to be satisfactory, the risk category may be downgraded to Low Risk. However, if any suspicious activity is observed based on client-provided information or transaction patterns, the risk category may be upgraded to High Risk, subject to approval by the Internal Compliance Committee or the Compliance Officer, as applicable.

Low Risk Category Clients

All Retail Clients who may not fall in any of the categories mentioned above and are providing maximum information as per KYC & exhibit complete transparency, maybe classified as low risk clients:

Examples:

i. Salaried employees and their spouses
ii. Senior citizens / Retired persons
iii. Good Corporate / Firms / HNIs / Individuals having respectable social and financial standing
iv. Clients which have been introduced by Authorized Persons / branch managers and they have known them personally and have faith in their genuineness.

Post-registration due diligence shall be conducted on a regular basis, taking into account the transactions executed by such clients. Based on the review, if the client's transactions are found satisfactory, then it will be maintain in the Low Risk category. However, if any suspicious activity is observed based on client-provided information or transaction patterns, the risk category may be upgraded to Medium Risk or High Risk, subject to approval by the Internal Compliance Committee or the Compliance Officer, as applicable.

In case of Non- Individual clients to obtain:

a) Copy of Balance sheet for the last 2 financial years at the time of Account opening and to be submitted every year thereafter.
b) Copy of latest shareholding 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/ Managing director at the time of Account opening and to be submitted every year thereafter.

General rules-

The Company shall maintain a record of all transactions, the nature and value of which have been prescribed under the Rules notified under the Prevention of Money Laundering Act (PMLA). Such transactions shall include all suspicious transactions, including, *inter alia*, credits or debits to or from any non-monetary accounts such as demat accounts or securities accounts maintained by the registered intermediary.

Further, where identity records of existing clients are not available, the same must be obtained without delay. In case the client fails to furnish the required KYC documents within the stipulated time, the account shall be suspended or closed after giving due notice to the client.

Reasons for Suspicious:

Identity & verification of client

Internal parameters as defined at Track wizz Software

Activity in Accounts

Internal parameters as defined at Trackwizz Software

Nature of Transactions

Internal parameters as defined at Trackwizz Software

Value of Transactions –

Internal parameters as defined at Trackwizz Software.

Suspicious Transaction monitoring, identification, assessment and reporting:

A **Suspicious Transaction** means a transaction, whether or not made in cash, which to a person acting in good faith gives rise to **reasonable grounds of suspicion**. Such suspicion may arise where the transaction or activity:

- Is of **unusual or unjustified complexity**; or
- Appears to have **no economic rationale or bona fide purpose**; or
- Gives rise to suspicion that it **involves the proceeds of crime**, or is connected with **illicit or illegal activities**, including attempts to disguise the origin of such proceeds.

Monitoring and Reporting of Suspicious Transactions

- All transactions carried out within the organization shall be **subject to ongoing monitoring**.
- The responsibility for monitoring transactions shall vest with the **respective functional / departmental heads**, in line with their roles and responsibilities.
- Any alert generated by the surveillance system or any transaction observed to be suspicious shall be **reported immediately** to the **Compliance Officer / Principal Officer** for further examination and necessary action, in accordance with the provisions of PMLA and SEBI AML–CFT guidelines.

Criteria for ascertaining/identification of suspicious transaction Broking Division:-

Assessment of Suspicious Transactions

Whether a particular transaction is suspicious shall depend on the overall facts and circumstances, including but not limited to:

- Client background and relationship if any with the underlying company, its KMP & other RTO (Regulated Transaction Order) as may be issued by the FIU-IND under PMLA directing a Reporting Entity to regulate or restrict certain transactions to mitigate money laundering or terrorist financing risks.
- Nature and details of transactions
- Identity, receipt, and payment patterns

Key Indicators for Identifying Suspicious Transactions

The following factors may indicate suspicious or unusual activity:

- **Unusually large transactions**, such as clients trading in a particular scrip/share beyond a defined quantity or value threshold in a single day, or where the client's volume exceeds a specified percentage of the total exchange volume in that scrip.
- **Client's relationship** with the company, its directors, or promoters in relation to the scrips traded.
- **Difficulty in client identity verification**, including cases of non-cooperation by the client.
- **Inconsistencies in transactions** with respect to volume, delivery, financial standing, KYC details, or other related parameters.

Dormant Accounts

- Trading accounts in which no transactions have been carried out for the last 24 months and which do not have any outstanding positions in F&O or CDS shall be treated as **Dormant Accounts**.
- A defined **reactivation procedure** shall be followed for such dormant broking accounts.

Trading in Illiquid Securities
In cases where a client has executed transactions in illiquid securities (e.g., Z, X, XT Group securities, Trade-to-Trade (T2T) category securities, etc.):

- Transaction-related alerts shall be reviewed in accordance with the **Company's Risk Management Policy and/or Surveillance Policy**.
- Reviews shall be based on parameters defined in the **TrackWizz system**.

Enhanced Monitoring – S+ Framework Securities
In case of **S+ framework securities**, including:

- **"SS"** – Securities settled on a normal rolling basis
- **"ST"** – Securities settled on a trade-to-trade basis

Enhanced due diligence shall be carried out through **increased monitoring**, including trading in identified securities either by MEL in its own account or on behalf of clients.

Criteria for ascertaining/identification of suspicious transaction Depository Division:

Alerts generated by CDSL based on transactions in Depository Accounts on following parameters:

- Debit and Credit transactions due to Off-market or Inter-depository transfers, above a threshold quantity, in an ISIN, in a single transaction or series of transactions executed during the fortnight.
- Details of debit and credit transactions due to Demat remat and pledge (all categories) above a threshold quantity / value, in an ISIN, in a single transaction or series of transactions executed during the fortnight.
- Details of debit and credit transactions above a threshold quantity/value Whichever is smaller, in an ISIN, which exceed a threshold multiple of the average size of the transaction calculated for the previous months' transactions.
- Details of Off-market transactions (within CDSL or Inter-depository) where there are more than a threshold number of transactions in an account, for the past fortnight.
- Any debit transaction in a dormant account for exceeding a threshold Quantity/value whichever is smaller, are reported as an alert. An account having no 'Debit' Transaction in the last 6 months is considered as dormant account for this purpose**.**

The surveillance official will generate the suspicious transaction alert and inspect all alerts to come to the conclusion, regarding which alert (based on gravity of the case) should move to investigation/ assessment purpose.

The final alerts should be investigated & the report should be submitted to Compliance officer/ principal officer. The Compliance/Principal Officer will scrutinize all the alerts & report sent to him. After coming to the conclusion by Compliance/Principle officer, the decision for submitting the report or filing the STR will be taken on case-to-case basis. As the business dynamics are very dynamic & complex, defining the transaction for reporting will be on the sole discretion of Compliance officer/ principal officer, after come to the conclusion.

Risk Assessment

The company 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 shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions (these can be accessed at Securities and Exchange Board of India)

Clients/ customers from high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, shall have an 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.

Reporting

In case of suspicion observed for any /some of the client or group then there shall be continuity in dealing with the clients as normal and the client shall not be told of report/suspicion. However, in certain cases based on the gravity & nature of transaction, the principal officer based on its observation (backed by facts) may discontinue the operations in the account and may suspend any or all the transactions.

While reporting the suspicious transaction, the principle officer shall provide all the details including the cases where transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. The principal officer shall report all such attempted transactions in STRs irrespective of the amount of the transaction.

Filing of CTR & STR

The principal officer will file/submit Cash Transaction Report (CTR) (wherever applicable) for each month to FIU-IND by 15th of the succeeding month. The principal officer will file/submit Suspicious Transaction Report (STR) 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.

Utmost confidentiality are to be maintained while filing of CTR and STR to FIU-IND.

WEAPONS OF MASS DESTRUCTION (WMD):

The section relates to compliance obligations under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"), as well as directives issued by SEBI and the Government of India.

1. Purpose and Legal Basis

- The SEBI circular (dated April 26, 2023) and the Ministry of Finance order (dated January 30, 2023) require all intermediaries (such as brokers, depositories, and other regulated entities) to follow strict procedures to prevent financing or facilitation of activities related to weapons of mass destruction or their delivery systems.

- This obligation arises under Section 12A of the WMD Act, which gives the Central Government the authority to act against anyone involved in financing or supporting prohibited WMD activities.

2. Government Powers under Section 12A

- The Central Government can:
  - Freeze, seize, or attach any funds, financial assets, or economic resources belonging to individuals or entities associated with WMD-related activities.
  - Prohibit any person from providing money, financial assets, services, or economic resources that could benefit such individuals or entities.
- These actions are taken to prevent financing of terrorism or proliferation of weapons of mass destruction, as mandated under the WMD Act and related international obligations such as the UN Security Council Resolutions.

3. Obligations of MEL

- MEL will ensure full compliance with these requirements and take immediate action if any of its clients or counterparties are identified as designated individuals/entities (those listed by the Government or UN under WMD sanctions lists).
- In such a case, MEL will:

  - Report immediately the full details of the identified client, including all related funds, securities, or financial assets held with MEL.
  - 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 Chief Nodal Officer ("CNO"). The details of the CNO are as under:

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

    Nodal Officer of SEBI, Deputy General Manager, Division of FATF,
    Market Intermediaries Regulation and Supervision Department, to
    Securities and Exchange Board of India,
    SEBI Bhavan II, Plot No. C7, "G" Block,
    Bandra Kurla Complex, Bandra (E),
    Mumbai 400 051. email (sebi_uapa@sebi.gov.in)

4. Purpose of Reporting

Reporting has to be done to the competent authorities such as Chief Nodal officer of FIU-INDIA and SEBI as to prevents or prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act

- *for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.*

Designated Director and Principal Officer – Roles and Responsibilities

In accordance with the provisions of the Prevention of Money Laundering Act, 2002 (PMLA) and the SEBI Master Circular on AML/CFT standards, the Company shall appoint a Designated Director and a Principal Officer to ensure overall compliance with the AML/CFT framework.

The Designated Director shall be responsible for ensuring that the Company complies with all obligations under the PMLA and the Rules framed thereunder. The Designated Director shall oversee the formulation, implementation, and periodic review of AML/CFT policies and procedures, and shall ensure that adequate internal controls are in place to prevent money laundering and terrorist financing activities.

The Principal Officer shall act as the central point of contact between the Company, Financial Intelligence Unit – India (FIU-IND), SEBI, and other regulatory or enforcement agencies with respect to all AML/CFT-related matters.

Duties of the Principal officer-

1) The principal officer has legal obligations to report suspicious transactions to the authorities including FIU. The principal officer shall act as a central reference point in.

2) Facilitating onward reporting of suspicious transactions and an active role in the identification and assessment of potentially suspicious transactions and shall report to CEO at the next reporting level or the Board of Directors.

3) The Officer shall not impose any restrictions on the operation of client accounts merely on the basis of a Suspicious Transaction Report (STR) being filed, except in cases where the transactions involve any of the following:

- Fraudulent activities wherein the Company is the ultimate victim or sufferer;
- Transactions that distort the fair and efficient functioning of the market mechanism;
- Serious manipulative or deceptive transactions that compromise market integrity;
- Situations where the client is withdrawing funds or securities with an apparent intent to immediately close the account; or
- Instances where there exists a risk of distortion or tampering of material facts or evidence.

In such exceptional cases, the Officer may, after consultation with the Compliance Head and Designated Director, initiate appropriate restrictions and record detailed reasons for the action taken.

4) The officer shall ensure that no directors, officers and employees (permanent and temporary) shall be disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND.

Co-operation with Authorities

The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining client confidentiality. Confidential

information about clients may, therefore, only be given to the authorities when there is a legal obligation to do so.

The Company and its staff shall strictly ensure that there is no 'tipping-off' to clients about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a client, it may seriously hamper the enquiry/investigation of the authorities.

There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

Investors Education:
Implementation of AML and CFT measures requires the Company to obtain certain personal or financial information from clients, such as proof of funds, income tax returns, or bank statements. Clients may question the need for such details; hence, it is important to explain that these requirements arise from regulatory obligations under PMLA and SEBI guidelines. The information is collected solely for compliance purposes and is handled with strict confidentiality.

Employee Awareness and Training on AML / CFT

The Company shall put in place an ongoing Employee Training Program to ensure that all staff members, particularly those dealing directly or indirectly with clients and financial transactions, are adequately trained in Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations.
The training program shall cover topics such as:

- The provisions of the Prevention of Money Laundering Act, 2002 (PMLA) and the Rules framed thereunder;
- SEBI and Exchange guidelines on AML/CFT compliance;
- Methods of identifying suspicious transactions and unusual patterns of client behavior;
- Procedures for reporting Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs); and
- The importance of maintaining confidentiality while handling client and transaction information.

MEL conducts comprehensive AML training program periodically (i.e., quarterly or half-yearly) to ensure a thorough understanding of the PMLA regulations among all new and existing employees.

Special refresher training sessions shall be conducted whenever there are changes in regulatory requirements or when new typologies of money laundering or terrorist financing are identified.
The Principal Officer and the Compliance Officer ensure that the training modules are updated on a regular basis and that employee participation is properly documented and monitored.
Employees are required to formally acknowledge their understanding of MEL's AML/CFT policies and procedures. Any instances of non-compliance or negligence in complying with these guidelines shall be monitored and escalated to the appropriate authority.

Recruitment of personnel

The Human Resources (HR) Department shall ensure thorough background verification of all employees prior to recruitment. Adequate safeguards must be taken to establish the authenticity and genuineness of the individual being recruited and maintain documentary evidence of such verification in the employee's personnel file.

The HR Department shall obtain and verify the following documents from each employee at the time of recruitment:

1. Recent Photograph
2. Proof of Address
3. Proof of Identity
4. Proof of Educational Qualification
5. References (professional or personal, as applicable)
6. Verification through Surveillance Application

All employee-related documents shall be securely maintained and preserved in accordance with the Company's record retention policy. Access to such information shall be restricted to authorized personnel only.

Retention of records

The Company shall maintain and preserve all records pertaining to clients and their transactions in accordance with the provisions of the Prevention of Money Laundering Act, 2002 (PMLA), the Rules framed thereunder, and relevant SEBI and Exchange guidelines.
The records to be maintained shall include:

- All transactions undertaken by clients;
- Documents evidencing the identity of clients and their beneficial owners;
- Information relating to client transactions, whether attempted or executed; and
- Details of reports or information submitted to the Financial Intelligence Unit – India (FIU-IND).

We are maintaining detailed records of transactions such as client identification and account files for a five years after the business relationship has ended or the account has been winded-up. These retention of data are to be maintained for securing the data for future audit and investigations. The Client exact nature of the information been maintained, including the nature of transactions, amount and currency, date of transaction, and parties involved.

In accordance with SEBI Circular No. SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18, 2020, Mehta Equities Ltd. (MEL), as a Depository Participant, shall preserve all records and documents for a minimum period of eight (8) years, in their original form, either in physical or electronic mode. Copies of such records shall be made available to any enforcement or regulatory agency during the course of inspection or investigation, as required.

While maintaining records, all types of transactions shall be considered, including:

- Transactions integrally connected to one another;
- Transactions remotely connected or related; and
- Any other activity or transaction that may reasonably be classified as suspicious or unusual.

Further, records pertaining to active clients and staff details collected during the recruitment process are being preserved securely. Such information shall be maintained in safe custody, with

restricted access provided only to authorized personnel. Adequate safeguards being implemented to prevent unauthorized access, alteration, or destruction of these records.

Review of the policy-

AML policy is to be well documented and reviewed on a regular basis, taking into account the outcomes of risk assessment exercises arises from AML alerts.
The AML Policy shall be reviewed by the Principal Officer in consultation with one of the Directors. The outcome of this review shall be presented to the Board, or to any committee of the Board to which such powers have been delegated, and subsequently placed before the Board for approval. The policy shall be reviewed at least annually.

****