

PMLA POLICY

Smart Equity Brokers Private Limited

Approved by Board on July 19, 2024

Introduction of Smart Equity Brokers Private Limited

Smart Equity Brokers Private Limited (SEB) is a member of National Stock Exchange of India Limited, BSE Limited and Multi Commodity Exchange of India Limited (MCX) having SEBI Regn No. INZ000177636. SEB is also a depository Participant of NSDL vide SEBI Regn No.: IN-DP-NSDL-276-2016.

This Prevention of Money Laundering policy has been prepared in accordance Prevention of Money Laundering Act, 2002 (PMLA Act). This policy also takes into account the provisions of PMLA Act, Master circular issued by SEBI on June 06, 2024 and rules laid down by FIU.

Section 1: Overview

1.1 Introduction and Background of AML

SEBI has issued necessary directives vide circulars from time to time, covering issues related to Know Your Client (KYC) norms, Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

The Directives given by SEBI are intended for the use primarily by intermediaries registered under Section 12 of the SEBI act 1992. The overriding principle is that the intermediaries should be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA .The PMLA has been further amended vide notification dated March 06,2009 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 SEBI Act 1992 will now be treated as a scheduled offence under Schedule B of PMLA.

On June 06, 2024 a master circular no. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 consolidating all the requirements/ instructions has been issued by SEBI which supersedes all the earlier circulars. As per the provisions of PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (Maintenance of Records Rules), as amended from time to time and notified by the Government of India, every reporting entity (which includes intermediaries registered under section 12 of the SEBI Act, i.e. a stock-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the SEBI Act and stock exchanges), shall have to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

1.2 Policies and procedures to combat Money Laundering and Terrorist Financing.

1.2.1 Obligation to establish policies and procedures: -

- a) Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all intermediaries ensure the fulfillment of the aforementioned obligations.
- b) To be in compliance with these obligations, the senior management shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Company shall: -

- i) issue a statement of policies and procedures, where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
- ii) ensure that the content of these Directives are understood by all staff members;
- iii) regularly review the policies and procedure to ensure their effectiveness;
- iv) adopt client acceptance policies and procedures
- v) 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;
- vi) have system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities
- vii) develop staff members awareness and vigilance to guard against ML and TF;

1.2.2 Policies and procedures to combat ML shall cover: -

- a) Communication of company policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
- b) Client acceptance policy and client due diligence measures, including requirements for proper identification;
- c) Maintenance of records;
- d) Compliance with relevant statutory and regulatory requirements;
- e) Co-operation with the relevant law enforcement authorities including timely disclosure of information;
- f) Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard.
- g) The Internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure and number of clients and other such factors.

Section 2: Detailed Directives

2.1 Vision towards Anti Money Laundering

- 2.1.1** Smart Equity Brokers Private Limited (The Company) has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a frame-work to report suspicious transactions to FIU as per the guidelines of PMLA Rules, 2002 and as prescribed by SEBI vide its Circular No. SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated July 04, 2018.
- 2.1.2** The Company does not deal in cash except in Depository division, where client makes payment of small amount for Annual maintenance of Depository account and other transaction charges; normally amount ranging Rs.500 to Rs.1000. Hence the requirement of maintaining record of cash transaction in excess of Rs.10 Lakh is ruled out.
- 2.1.3** For suspicious transactions whether or not made in cash, we observe the trading pattern of the client on difference criteria like quality of scrip, market participation, Income & Networth, funds received, trading behavior etc.
- 2.1.4** Compliance department of the company review & update PMLA policy on time to time based on the circular issued by regulator in consultation with Principal Officer.

2.2 Client Due Diligence (CDD)

2.2.1 The CDD measures comprise the following:

- (a) Obtaining sufficient information in order to identify person 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 are identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
- (b) Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person. Provided that in case of a Trust, the company shall ensure that trustees disclose their status at the time of commencement of an account based relationship.
- (c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted. The beneficial owner shall be determined as under-

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

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

- "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;

- ii. **where the client is a partnership firm,** the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than ten per cent 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;

- iii. **where the client is an unincorporated association or body of individuals,** the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;
- iv. where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
- v. **For client which is a trust:** the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
- vi. 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.

- vii. **Applicability for foreign investors:** where the SEB is dealing with foreign investors' 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, shall be taken into account;

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

- (d) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c).
- (e) Understand the nature of business, ownership and control structure of the client;
- (f) Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the Smart Equity Brokers Private Limited knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.
- (g) 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, 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.
- (h) Periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process
- (i) In case of client being a non-profit organization, register the details of a client, 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.
- (j) In case of suspicious transactions that relates to money laundering or terrorist financing, and it is reasonably believed that performing the CDD process will tip-off the client, the CDD process shall not be pursued, and instead STR shall be filed with FIU-IND.

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

2.2.2 Policy for acceptance of clients:

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. To apply client due diligence on a risk sensitive basis depends on the type of client business relationship or transaction.

The following safeguards shall be followed by the company while accepting the clients:

- a) No opening of or keeping of any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified, shall be allowed.
- b) 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 include the following:

- (i) Non-resident clients;
- (ii) High net worth clients;
- (iii) Trust, Charities, NGOs and organizations receiving donations;
- (iv) Companies having close family shareholdings or beneficial ownership;
- (v) Politically exposed persons (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 paragraph 20 of the Master Circular on 'Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under', dated February 3, 2023, shall also be applied to the accounts of the family members or close relatives / associates of PEPs;
- (vi) Clients in high risk countries. While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. The Company shall specifically apply Enhanced Due Diligence (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;
- (vii) Non face to face clients;
- (viii) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the company shall

exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

- c) Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.
- d) Ensure that an account is not opened where the company is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non - cooperation of the client in providing full and complete information. In such a case, the company shall not continue to do business with such a person and file a suspicious activity report. The company shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The company shall be cautious to ensure that it does not return securities or money that may be from suspicious trades. However, the company shall consult the relevant authorities in determining what action it shall take when suspicious trading is suspected.
- e) The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons i.e. the agent- client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.
- f) Do not accept clients with identity matching with a person known to have criminal background: Check whether the client's identity matches with any person known to be having criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory agency worldwide. If yes, we do not open the client account. Further, obtain undertaking from the client in this regard.
- g) Each client should be met in person: We have to perform the in person verification process very diligently. Either the client should visit the company/business associates office or concerned official/business associates may visit the client at their residence / office address. Official/Business associates also verify photocopy of the documents with the original. As far as possible, try to open account of known person or person introduced by an existing client. Further, we also capture the introducer detail in account opening form.
- h) Accept clients on whom we are able to apply appropriate KYC procedures: Obtain complete identification information from the client. It should be ensured that the initial forms taken by the client are filled in completely. All photocopies submitted by the client should be checked against original documents without any exception. 'Know Your Client' guidelines should be followed without any exception. All supporting documents as specified by Securities and Exchange Board of India (SEBI) and Exchanges should be obtained and verified.

- i) Do not compromise on submission of mandatory information/ documents: Client's account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Accounts where the client refuses to provide information/documents should not be opened. We shall capture data of key person like director & shareholder of all non-individual clients & also taking complete details/documents of Director/ Trustee/ Partners etc mandatory while opening the account. In case of corporate client in order to identify client with cross holding, we capture key person data like details of director, shareholder.
- j) Verify and Validate circumstances under which the client is permitted to act on behalf of another person/ entity are clearly laid down. It is specified in what manner the account should 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 Smart Equity Brokers Private Limited, as well as the person on whose behalf the agent is acting is clearly laid down). Adequate verification of a person's authority to act on behalf the client is also carried out.
- k) The CDD process shall necessarily be revisited, if required, when there are suspicions of money laundering or financing of terrorism (ML/FT).

2.2.3 Risk-based Approach:

2.2.3.1 The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

2.2.3.2 It is generally recognized that certain clients may be of a higher, medium or lower risk category depending on the circumstances such as the client's financial background, type of business relationship or transaction etc. As such, the company 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 other risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

2.2.3.1 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.

2.2.3.2 Risk Assessment

- a) 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.
- b) 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.

- c) The Company 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, if any. The Company shall ensure:
- d) The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions (these can be accessed at the URL http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>).

2.2.3.3 Risk Classification

The company should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as low risk, medium risk and high risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence.

Special attention must be paid to the transactions which are complex, unusually large or pattern which appears to have no economic purpose. Risk profiling is to divide into two broad categories one is on-board risk & second is ongoing risk. On-board risk is defined when a client is introduced to the company.

Risk categorization of client will be based on following parameters:

- a) If the client's location (registered office address, correspondence address) is out of India and in any of the high risk jurisdictions as defined by FATF.
- b) Individual Client having annual income more than Rs. 1 Crores and/or Networth of Rs. 25 Crores.
- c) *Income & Networth does not commensurate with transactions* (Trading/ DP).
- d) Client dealing in Forex.

Category will be assigned based on the following criteria:

- a) High - Meets all four parameters.
- b) Medium - Meets three parameters
- c) Low - Meets two or less

Special category customers & clients reported to FIU shall also move to the high risk category.

2.2.4 Client identification procedure:

2.2.5.1 Requirements of a Client Identification Procedure (CIP):

- a) The company shall proactively put in place appropriate risk management systems to determine whether our 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 as outlined in clause 2.2.5 shall also be applicable where the beneficial owner of a client is PEP.
- b) The company shall obtain approval from Principal Officer/ Designated Director 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, Principal Officer/ Designated Director's approval is mandatory to continue the business relationship.
- c) The company shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
- d) 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.
- e) The information must be adequate enough to satisfy competent authorities (regulatory/ enforcement authorities) in future that due diligence was observed by the SEB in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- f) Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority (Principal Officer).

2.2.5.1 SEBI has prescribed the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Company shall frame its own internal directives based on its experience in dealing with its clients and legal requirements as per the established practices.

Further, the company 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 intermediary is aware of the clients on whose behalf it is dealing.

2.2.5.2 The company 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 it considers appropriate to enable it to determine the true identity of its

clients.

2.2.5.3 It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to SEB from obtaining the minimum information/ documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly implemented and non-compliance shall attract appropriate sanctions.

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

2.2.6.1 The company may rely on a third party for the purpose of:

- a) Identification and verification of the identity of a client and
- b) Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

2.2.6.2 Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules.

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

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

2.3 Record Keeping

2.3.1 The company 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.

2.3.2 The company shall maintain such records as are sufficient to permit

reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

2.3.3 Should there be any suspected related to 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 our clients in order to maintain a satisfactory audit trail:

- a) the beneficial owner of the account;
- b) the volume of the funds flowing through the account; and
- c) for selected transactions:
 - i. the origin of the funds
 - ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
 - iii. the identity of the person undertaking the transaction;
 - iv. the destination of the funds;
 - v. the form of instruction and authority.

2.3.4 The Company shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

2.3.5 The Company shall put in place a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules as mentioned below:

- a) all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;
- b) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
However, for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.
- c) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- d) all suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the company.

Where there is no record of the identity of existing clients, the company shall obtain the records forthwith, failing to which the company shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of

clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

In case of transactions where any investigations by any authority have been commenced and in the case of transactions, which have been the subject of suspicious transactions reporting, all the records shall be maintained till the authority informs of closure of the case.

2.4.1 Information to be maintained

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

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

2.5 Retention of Records

2.5.1 We have 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 the company.

2.5.2 As stated in sub-section 2.2.5, we implement 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 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 has ended or the account has been closed, whichever is later.

2.5.3 Thus the following document retention terms shall be observed:

- a) All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed thereunder as well SEBI Act) and other legislations, Regulations or exchange bye-laws or circulars.
- b) The company shall maintain and preserve the records of documents evidencing the identity of its clients and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of five years after the business relationship has ended or the account has been closed, whichever is later.

2.5.4 In case of transactions where any investigations by any authority have been commenced and in the case of transactions, which have been the subject of suspicious transactions reporting, all the records shall be maintained till the authority informs of closure of the case.

- 2.5.5 **Records of information reported to the Director, Financial Intelligence Unit – India (FIU – IND):** The company shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, 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.

2.6 **Monitoring of transactions**

- 2.6.1 Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if we have an understanding of the normal activity of the client so that it can identify deviations in transactions/ activities.
- 2.6.2 The company 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 are required to be maintained and preserved for a period of five years from the date of transaction between the client and the company.
- 2.6.3 The company shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transaction 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 Principal Officer/ Designated Director.
- 2.6.4 Further, the compliance cell shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.
- 2.6.5 All transaction alerts generated by Exchange(s) will be monitored by Principal Officer for necessary action to be taken.

2.7 **Suspicious Transaction Monitoring and Reporting**

- 2.7.1 The company 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, the company shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.
- 2.7.2 A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:
- a) Clients whose identity verification seems difficult or clients that appear not

to cooperate

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

2.7.3 Any suspicious transaction shall be immediately notified to the Principal Officer. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature/ reason of suspicion. However, it 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 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.

2.7.4 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.

2.7.5 Clause 2.2.4 (g) of 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.

2.8 List of Designated Individuals/ Entities

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

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-releases>. 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.

The company shall ensure that accounts are not opened in the name of anyone whose name appears in said list. The company 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.

Further, maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them. The company shall also leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

The company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA

Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to 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.

The company 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.

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

2.9.1 The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, the Company does 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).

- 2.9.2 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. A corrigendum dated March 15, 2023 has also been issued in this regard. The list of Nodal Officers for UAPA is available on the website of MHA.

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

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

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

“(2) For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

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

- (i) owned or controlled, wholly or jointly, directly or indirectly, by such person; or
- (ii) held by or on behalf of, or at the direction of, such person; or
- (iii) derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

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

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

- 2.10.3 The Company is directed to comply with the procedure laid down in the said Order.

2.10.4 The company shall:

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

- (c) 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, the company 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;
- (d) send a copy of the communication, mentioned in paragraphs III(ii) and IV(iii) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051;
- (e) 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;
- (f) file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs IV(ii) and (iii) above, carried through or attempted through.

2.10.5 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.

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

2.11 Reporting to Financial Intelligence Unit-India

- 2.11.1 In terms of the PML Rules, the company is required to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU- IND) at the following address:

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

- 2.11.2 The company shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format (https://fiuindia.gov.in/files/downloads/Filing_Information.html). 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:

- a) The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- b) The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
- c) The Non-Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month.
- d) The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;
- e) Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.
- f) No nil reporting needs to be made to FIU-IND in case there are no

suspicious transactions to be reported.

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

2.11.4 We shall not put any restrictions on operations in the accounts where an STR has been made. We, our 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.

Further, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, the company shall file STR if it has reasonable grounds to believe that the transactions involve proceeds of crime.

2.12 Appointment of Principal Officer

To ensure that Company properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the Identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU.

Accordingly, we have appointed Mr. Arun Khera as the principal officer and his appointment has been duly informed to Director-FIU.

2.13 Appointment of Designated Director

We have appointed Mr. Arun Khera as Designated Director of the Company and his appointment has been duly informed to Director-FIU. His rights and duties comprise compliance with the obligations imposed under rules and regulations.

2.14 Guidelines for Employees Hiring/ Employees Training/Investor Education.

Hiring of Employees: The company shall have adequate screening procedures in place to ensure high standards while hiring employees.

Training of Employees: The company shall ensure to have regular training programmes, where the staff members (front office, back office, compliance, risk management staff and staff dealing with new clients etc) are updated about the AML and CFT procedures.

Investor Education: To implement AML/ CFT measures, at times we may be required to collect certain information from investors which may be of personal in nature or has hitherto never been called including documents evidencing source of funds/ income tax return/bank records etc. and can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. To address these queries we must sensitize and educate our clients about these requirements. For this, we shall circulate the PMLA Circulars and other specific literature/pamphlets etc. so as to educate the client of the objectives of the AML/CFT program.

This policy has been approved by the Board of Directors of the Company and will be reviewed as and when need arises and in any case once a year.