

Policy	Policy and Procedures to be implemented for PMLA & Implementation of AML/ CFT measures
Policy Version	7
Policy review date	May 28, 2024
Policy reviewed by	Compliance Head
Approval Authority	Board of Directors
Policy approved by Board on	May 28, 2024
Officer responsible for implementation	Compliance Officer and Operational Staff

**Table of Contents:**

<b>Topic</b>	<b>Page No.</b>
Introduction	1
Overview	2
Background	2 - 3
Policies and Procedures to Combat Money Laundering and Terrorist financing	3 - 5
Client Due Diligence (CDD)	5 - 8
Policy for acceptance of clients	8 - 11
Client identification procedure	11 - 13
Risk Management	13 - 14
Monitoring of Transactions	14 - 15
Suspicious Transaction Monitoring and Reporting	15 - 17
Record Management	17 - 20
List of Designated Individuals/ Entities	20 - 22
Jurisdictions that do not or insufficiently apply the FATF Recommendations	22
Reporting to Financial Intelligence Unit - India	22 - 24
Designation of officers for ensuring compliance with provisions of PMLA	25 - 26
Hiring and Training of Employees and / Investor Education	26 - 27

**1. Introduction:**

The Prevention of Money Laundering Act, 2002 (“PMLA”) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (Maintenance of Records Rules<sup>1</sup>), as amended from time to time and notified by the Government of India, mandate every reporting entity [which includes intermediaries registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) and stock exchanges], to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities. The Maintenance of Records Rules, inter alia, empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the Maintenance of Records Rules and for furnishing information thereof, in such form as may be directed by the regulator.

The enclosed policy stipulates the essential principles for combating Money Laundering (ML) and Terrorist Financing (TF) and provides detailed procedures and obligations to be followed and complied with by Unique Stockbro Pvt Ltd (hereinafter referred to as “Unique or Company” as the case may be) as a registered intermediary.

This policy shall apply to all operations conducted by Unique.

SEBI has from time to time issued circulars/ directives with regard to Know Your Client (KYC), Client Due Diligence (CDD), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) specifying the minimum requirements. It is emphasized that the registered intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

The earlier policy will be superseded on implementation of this policy.

## **2. Overview**

- i. The Policy as outlined below provide a general background and summary of the main provisions of the applicable anti-money laundering and anti-terrorist financing legislations in India. It also provides guidance on the practical implications of the Prevention of Money Laundering Act, 2002 (PMLA). The Policy also sets out the steps that Unique or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities.
- ii. This Policy is prepared after taking into consideration factors such as the specific nature of our business, organizational structure, type of clients and transactions, etc. The overriding principle is that the company shall be able to satisfy itself 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.

## **3. Background**

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.

The Maintenance of Records Rules empower SEBI to specify the

information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by the regulator for detecting the transactions specified in the Maintenance of Records Rules and for furnishing information thereof, in such form as may be directed by SEBI.

4. The PMLA inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as provided in Section 12A read with Section 24 of the SEBI Act will be treated as a scheduled offence under schedule B of the PMLA.

### **Policies and Procedures to Combat Money Laundering and Terrorist Financing**

#### **Essential Principles:**

5. This Policy has taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed Policy has outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. The policy has been prepared after having regard to the specific nature of business, organizational structure, type of client and transaction, etc. and to satisfy us that the measures taken are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.
- 5A. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform SEBI.

**Obligation to establish policies and procedures**

6. 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 registered intermediaries ensure the fulfilment of the aforementioned obligations.
- 6A. "group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of rule 2 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 as amended from time to time.
7. To be in compliance with these obligations, the senior management of the company 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 and implement, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
  - ii. ensure that the content of these Policy are understood by all staff members;
  - iii. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness.
  - iv. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
  - v. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

- vi. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
- vii. develop staff members' awareness and vigilance to guard against ML & TF.

### **Client Due Diligence (CDD)**

**8. The CDD measures comprise the following:**

- i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/ or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;
- ii. Verify the client' identity using reliable, independent source documents, data or information

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

- iii. Identifying beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted. The beneficial owner shall be determined as under-
  - a) **Where the client is a company:** The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation: for the purpose of this sub-clause:

- I. "Controlling ownership interest" means ownership of or entitlement to more than **ten per cent of shares or capital or profits** of the company;
  - II. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders' agreements or voting agreements;
- b) **Where the client is a partnership firm:** The beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation: For the purpose of this clause:

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

- c) **Where the client is an unincorporated association or body of individuals:** The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent of the property or capital or profits of such association or body of individuals;
- d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
- e) **Where the client is a trust:** The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any



other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

- f) Where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- g) **Applicability for foreign investors:** This will be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client
- h) Company shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through its Board of Directors.
- iv. 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
- v. Understand the ownership and control structure of the client;
- vi. 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 Company's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;
- vii. The Company shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities

relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data

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

### **Policy for acceptance of clients**

9. The following safeguards are to be followed while accepting the clients:

- i. The Company shall not allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified;
- ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile
- iii. The Company shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:
  - a) Non - resident clients;

- b) High net-worth clients;
- c) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations;
- d) Companies having close family shareholdings or beneficial ownership;
- e) Politically Exposed Persons” (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. The additional norms applicable to PEP as contained in the subsequent paragraph 14 of the master circular shall also be applied to the accounts of the family members or close relatives / associates of PEPs;
- f) 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, the Company 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](http://www.fatf-gafi.org)) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude Company from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas;

The Company shall specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which

this is called for by the FATF.

- g) Non face to face clients. Non face to face clients means clients who open accounts without visiting the offices of the Company or meeting the officials of the Company.
- h) Clients with dubious reputation as per public information available etc.
- iv. Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Policy and Circulars issued by SEBI from time to time.
- v. 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 - co-operation of the client in providing full and complete information. The Company shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The 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 it suspects suspicious trading.
- vi. 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.

- vii. Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.
- viii. The CDD process shall necessarily be revisited when there are suspicions of ML/TF.

### **Client identification procedure**

- 10.** Client identification procedure (CIP) to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.
- 11.** Company shall be in compliance with the following requirements while putting in place a CIP:
  - i. The Company will determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.
  - ii. Company is required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Company shall obtain senior management approval to continue the business relationship.
  - iii. 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.

- iv. The client shall be identified by the Company by using reliable sources including documents / information. The Company shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
  - v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the Company in compliance with the policy. Each original document shall be seen prior to acceptance of a copy.
  - vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the Company.
- 12.** SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time. The Company will fulfil these minimum requirements and also enhance the same depending upon each case.
- 13.** 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, policy and circulars issued thereunder so that the Company is aware of the clients on whose behalf it is dealing.
- 14.** The Company will comply with the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to the Company 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 the Company.

## **Risk Management**

### **Risk-based Approach**

15. 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.
16. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, 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 the Company shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk- based approach, the type and amount of identification information and documents that Company shall obtain necessarily depend on the risk category of a particular client.
17. 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.

### **Risk Assessment**

18. 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.
19. 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.
20. 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. Company shall ensure.
21. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

### **Monitoring of Transactions**

22. Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the Company has an understanding of the normal activity of the client so that it can identify deviations in transactions/ activities.
23. The Company shall pay special attention to all complex unusually large transactions/ patterns which appear to have no economic purpose. The Company will pay special attention to transactions which exceeds regular 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/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

24. The Company shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.
25. The Company shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the Company.
26. Further, the compliance cell of the Company shall randomly examine a selection of transactions undertaken by clients to check on their nature i.e. whether they are in the nature of suspicious transactions or not.

### **Suspicious Transaction Monitoring and Reporting**

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

to cooperate;

- ii. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
- iii. Clients based in high risk jurisdictions;
- iv. Substantial increases in business without apparent cause;
- v. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- vi. Attempted transfer of investment proceeds to apparently unrelated third parties;
- vii. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

**29.** Any suspicious transaction shall be immediately notified to the Designated/Principal Officer within the Company. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

**30.** 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 Company shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction

- 31.** Paragraph 12 (iii) (f) of this Circular categorizes clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. 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.

## **Record Management**

### **Information to be maintained**

- 32.** Company is required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:
- i. the nature of the transactions;
  - ii. the amount of the transaction and the currency in which it is denominated;
  - iii. the date on which the transaction was conducted; and
  - iv. the parties to the transaction.

## **Record Keeping**

- 33.** Company shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.
- 34.** 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 behaviour.
- 35.** In case of any suspected laundered money or terrorist property, the competent

investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, Company shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

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

**36.** 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 thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

**37.** The Company shall not allow cash transaction for any client. The Company shall maintain proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

- i. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account all suspicious transactions whether or not made in cash and including, such as demat

account, security account maintained by the registered intermediary.

### **Retention of Records**

- 38.** Registered intermediaries shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.
- 39.** Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and the Company has ended or the account has been closed, whichever is later.
- 40.** In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.
- 41.** 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 between the client and the intermediary.
- 42.** Where the Company does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the Company shall close the account of the clients after giving due notice to the client.
- 43.** Explanation: For this purpose, the expression “records of the identity of clients” shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.
- 44.** Procedure for freezing of funds, financial assets or economic resources or related

services

45. Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, it 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).
46. In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2). A corrigendum dated March 15, 2023 has also been issued in this regard (Annexure 3). The list of Nodal Officers for UAPA is available on the website of MHA

#### **List of Designated Individuals/ Entities**

47. 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'. Company shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.
48. 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.
49. An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <https://press.un.org/en/content/press-release>. The details of the lists are as under:
- i. The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of

individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at:

<https://www.un.org/securitycouncil/sanctions/1267/press-releases>.

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

- 50.** Company will ensure that accounts are not opened in the name of anyone whose name appears in said list. 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.
- 51.** Company shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/ entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.
- 52.** The Company shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.
- 53.** 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.
- 54.** Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: [jsctcr-mha@gov.in](mailto:jsctcr-mha@gov.in).
- 55.** 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](mailto:sebi_uapa@sebi.gov.in)) to the UAPA nodal officer of SEBI, Deputy

General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, “G” Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

### **Jurisdictions that do not or insufficiently apply the FATF Recommendations**

56. FATF Secretariat after conclusion of each of its plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the Company.
57. The Company shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the Company is not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

### **Reporting to Financial Intelligence Unit-India**

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



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

59. 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](https://fiuindia.gov.in/files/downloads/Filing_Information.html)).

These documents contain detailed policy 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, Company shall adhere to the following:

- i. The Cash Transaction Report (CTR) is not applicable to the company as it does not allow cash transaction.
- ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

- iii. The Non-Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month.
- iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;
- v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.
- vi. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.
- vii. Non-profit organization” means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

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

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

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

**Designation of officers for ensuring compliance with provisions of PMLA**

**61. Appointment of a Principal Officer:** To ensure that the 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 email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

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

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

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

- a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
- b) the managing partner if the reporting entity is a partnership firm,
- c) the proprietor if the reporting entity is a proprietorship firm,
- d) the managing trustee if the reporting entity is a trust,
- e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

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

**63.** Company shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

### **Hiring and Training of Employees and Investor Education**

- a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
- b) the managing partner if the reporting entity is a partnership firm,
- c) the proprietor if the reporting entity is a proprietorship firm,
- d) the managing trustee if the reporting entity is a trust,
- e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
- f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above".

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

**65.** Training of Employees: The Company shall have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline

staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these policy, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

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

For & behalf of  
Unique Stockbro Private Limited

Principal Officer

Date: May 28, 2024

Place: Mumbai