TATA SECURITIES LIMITED

KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY LAUNDERING (PML) POLICY

PART A[1]

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.

I. Introduction:

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.

The objective of the directives is to prevent the registered intermediaries from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the registered intermediaries to know/understand their customers and their financial dealings better which, in turn, help them manage their risks prudently.

Based on the framework provided by the SEBI from time to time, a KYC - Prevention of Money Laundering (PML) policy has been formulated (hereinafter referred to as the "KYC - PML Policy").

The following are the four key elements of the Policy:

(i) Customer Acceptance Policy;
(ii) Risk Management;
(iii) Customer Identification Procedures; and
(iv) Monitoring of Transactions

As per the provisions of The Prevention of Money Laundering Act, 2002 ("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 Securities and Exchange Board of India Act, 1992 (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 of records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

[1] *The KYC-PML Policy is divided in 2 parts. 'Part A' deals with guidelines on Anti Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) issued by SEBI. 'Part B' deals with guidelines on Know Your Customer / Anti Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT) issued by Pension Fund Regulatory and Development Authority (PFRDA)*

II. Policies And Procedures for Implementation of PMLA

1) Policy objectives

- To prevent criminal elements from using our business for money laundering activities or the funding of terrorist or criminal activities.
- To understand the customers and their financial dealings better, which in turn would help us manage the risk prudently.
- To put in place appropriate controls for detection and reporting suspicious transactions in accordance with applicable laws/ laid down procedures
- To comply with applicable laws and regulatory guidelines.

2) Scope: These policies and procedures will apply to the operation of the Company in respect of businesses undertaken by it in its capacity of an intermediary registered with SEBI i.e. stock-broker and depository participant and are to be read in conjunction with the existing guidelines.

Any references in this policy to clients/customers are to be construed according to the definition of "Client", in PMLA. The terms 'client' and 'customer' have been used interchangeably herein.

3) Key Elements of the Policy:

i. No cash transactions:
The company will not enter into any cash transactions with clients for any reason whatsoever.

ii. Group-wide Policy:
The Company will put in place a group-wide programs against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programs shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(Group – The term "group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes, —

i. is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or

ii. would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident;

Group as per clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961.)

III. Important Guidelines issued by SEBI on AML CFT / Obligations of Securities Market Intermediaries under the PMLA and Rules framed there under.

Guiding Principles:

These guidelines have considered the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. These guidelines have outlined relevant measures and procedures to guide the registered intermediaries in preventing Money Laundering (ML) and Terrorist Financing (TF).

The Company shall consider carefully the specific nature of its business, organizational structure, type of customer and transaction etc. to satisfy itself that the measures taken by it are adequate and appropriate to follow the spirit of the suggested measures and the requirements as laid down in the Act.

Senior management of the Company will be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with the relevant legal and regulatory requirements.

The Company shall:

- 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.
- Establish effective internal procedures that serve to prevent and impede money laundering and terrorist financing and global measures to be taken to combat drug trafficking, terrorism and other organized serious crimes.
- Ensure that the content of these guidelines are understood by all staff members.
- Regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review should be different from the one who has framed such policies and procedures.
- Adopt customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing.
- Undertake customer due diligence measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction.
- Have a system in place for identifying, monitoring and reporting suspected Money Laundering and Terrorist Financing transactions to the law enforcement authorities and
- Develop staff members' awareness and vigilance to guard against money laundering and terrorist financing.

Written Anti Money Laundering Procedures:

Each registered intermediary should adopt written procedures to implement the anti money laundering provisions as envisaged under the Act. Such procedures should include client due diligence process covering policy for acceptance of clients, procedures for identifying the clients, transaction monitoring and risk management.

IV. Customer Due Diligence ("CDD") process:

SEBI has issued guidelines specifying the documents required to be verified and submitted for opening of accounts of the clients in respect of stock broking and depository participant operations. These Guidelines are also reiterated by BSE, NSE, CDSL and NSDL through their circulars which are quite exhaustive. These requirements have been adhered to.

In short, while opening accounts of individuals, the original documents relating to proof of identity, proof of residence, PAN card are obtained and verified by an official of the Company. Moreover 'in person verification' of the client is carried out by an official of the Company and this fact is recorded in the application form. While opening of accounts in respect of entities other than individuals- documents like Memorandum of Association, Articles of Association, Board Resolution, photographs of authorized signatories, etc. are obtained.

In addition to this, PAN card details are verified on the Income Tax website. Websites of SEBI (www.sebi.gov.in) and Watch out Investors (www.watchoutinvestors.com) are also checked, to verify whether the person/entity is prohibited from trading in securities.

The CDD measures comprise the following:

- Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using 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.

- Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

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

- 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 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.

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 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;

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 (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
v. 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
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: Registered intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client;
viii. The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

- 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 the above;

- Understand the ownership and control structure of the client; Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and

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

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

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

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

V. Customer Acceptance Policy:

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

  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:

  a. Nonresident clients;

  b. High net worth clients;

  c. Trust, Charities, NGOs and organizations receiving donations;

  d. Companies having close family shareholdings or beneficial ownership;

  e. 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 14 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;

  f. Companies offering foreign exchange offerings;

  g. 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) form countries for which this is called for by the FATF;

  h. Non face to face clients;

  i. Clients with dubious reputation as per public information available etc.

  The above-mentioned list is only illustrative and the Company will exercise independent judgment to ascertain whether new clients should be classified as CSC or not. Accounts which belong to the "CSC" will be flagged and precaution will be taken about their operation.

- The profile of clients has to be updated regularly.

- Information about the income range of the client is obtained on the specified column in the application form. This information should be subsequently used for monitoring whether the transactions of the clients are within the declared means and if the value of the transactions is increasing, the client should be asked to disclose the increasing sources.

- A thorough assessment should be carried out to ascertain whether the client is dealing with us on his own behalf or someone else is the beneficial owner. If there are doubts, before acceptance of the clients, thorough due diligence should be carried out to establish the genuineness of the claims of the clients. Secrecy laws shall not be allowed as a reason for refusal to disclose the true identity of the client.

- No client should be accepted where it is not possible to ascertain the identity of the client, or the information provided is suspected to be non-genuine, or if there is perceived non-cooperation of the client in providing full and complete information.

- If any of the above are encountered when dealing with an existing client, all business with the client must be suspended and a prompt report must be made to the Compliance Officer to enable him/her to file a suspicious activity report with the relevant authorities.

- In case of clients who want to act through agent under Power of Attorney, a notarized power of attorney issued in favor of parties other than TSL, should be obtained. Original of the POA should be verified. Care should be taken to ensure the genuineness of the client.

- While accepting FIIs/sub accounts as clients, reports in market / public knowledge regarding their investment behaviour (for e.g., whether they allow their investment vehicle to be used by others; whether they issue underlying participatory notes) should be considered.

- KYC forms prescribed by SEBI/stock exchanges/ Depositories, duly signed by the client should be obtained before acceptance of the clients.

- 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.

- The Company shall ensure that an account is not opened where the intermediary is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non - co-operation of the client in providing full and complete information. The 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 registered intermediary shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

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

- 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.

VI. Client Identification Procedure (CIP):

- Before opening the accounts, there should be personal interaction with the client.

- Before opening the accounts in case of companies any one of the following viz. main promoter / Managing Director / whole time director / key management person and in the case of partnership any one of the active partners should be met in person.

- Caution is to be exercised when identifying companies which appear to be 'shell companies' or 'front companies'. Shell/front companies are legal entities, which have no business substance in their own right but through which financial transactions may be conducted.

- In case of clients acting through Power of Attorneys, the Principal and Agent should come in person for the first time. Photos of both are to be obtained along with signatures on the photos. The KYC form, Member Constituent Agreement and the Risk Disclosure Document must compulsorily be signed by the client himself and not by the POA holder.

- Original of valid, un-expired Photo identity of individual/promoter/director to be verified by our official for identifying the client. Signature of the persons should be obtained on the photos. Photocopy of the proof should be taken by our official, who should also certify thereon about having verified it with the unexpired original.

- Original of valid, un-expired Photo identity of individual/promoter/director to be verified by our official for identifying the client. Signature of the persons should be obtained on the photos. Photocopy of the proof should be taken by our official, who should also certify thereon about having verified it with the unexpired original.

- In case of individuals, proof of identify (as prescribed by SEBI) should be established by way of any of the following documents (un-expired original document shall be verified)
    - PAN Card
    - Passport
    - Voter ID
    - Driving license
    - UID (Aadhar Card)

  PAN card details must be checked on the Income Tax website for all the cases where PAN card is obtained as proof of identity.

  Photocopy of the proof should be taken by our official who should also certify thereon about having verified it with the unexpired original.

- Any of the following address proof should be obtained (un-expired Original should be verified)
    - Passport
    - Voter ID
    - Driving license
    - Bank pass book
    - UID (Aadhar Card)
    - Latest Rent agreement
    - Ration card
    - Latest Flat maintenance Bill
    - Latest Telephone Bill
    - Latest Electricity Bill
    - Insurance policy

  Photocopy of the proof should be taken by our official who should also certify therein about having verified it with the unexpired original.

- In the case of joint account, the above procedure should be carried out for all the persons who hold the joint account.

- Where the client is a company, certified copy of the following documents shall be obtained
    a) certificate of incorporation
    b) Memorandum and Articles of Association
    c) Copies of the balance sheet for the last 2 financial years (Copies of annual balance sheet to be submitted every year)
    d) Copies of latest shareholding pattern, including list of all those holding more that 5% in the share capital of the company, duly certified by the company secretary/whole time director/MD (copy of updated shareholding pattern to be submitted every year)

e) Copy of resolution from the Board of Directors approving participation in equity / derivatives / debt trading and naming authorized persons for dealing in securities and power of attorney granted to its managers, officers or employees to transact on its behalf, and

f) Photographs of whole time directors, individual promoters holding 5% or more, either directly or indirectly in the shareholding of the company and of persons authorized to deal in securities.

g) Identification documents (identity and address) for the above as applicable to individuals in respect of managers, officers or employees holding an attorney to transact on its behalf.

- Exemption in case of listed companies:

  Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

- Care should be taken if the persons mentioned in the Memorandum and Articles of Association as promoters/first directors are different from the current promoters / directors. If the name/address of registered office has been changed, reasonable enquires should be made.

- Proof of address of the registered office of the company, being one of the relevant documents as in the case of individuals should also be taken .

- Where the client is a partnership firm, certified copy of the following documents
  a) registration certificate
  b) partnership deed and
  c) Identification documents (identity and address) as applicable to individuals in respect of partners, managers, officers or employees holding a Power of Attorney to transact on its behalf.
  d) Proof of address of the firm on the basis of relevant documents as applicable to individuals.

- Where the client is a trust, certified copy of the following documents;
  i) registration certificate
  ii) trust deed and
  iii) proof of identity and address of the trustees as applicable to the individuals.

- In the case of broking transactions, care should be taken to ensure that the orders are placed by the client and not by others on behalf of the client. If the client

proposes to authorize another person to place orders on his behalf, a properly executed Power of Attorney or Letter of Authority should be obtained and the person who will be placing orders shall also be identified using the above procedure. Periodical statement of accounts should be sent to the client (and not Power of Attorney holder) at his address mentioning that if he does not respond within 30 days of date of receipt of the letter, the contents shall be taken as approved.

- DP services should not be offered on a standalone basis (i.e. without broking relationship)

- After opening broking / DP accounts, a letter of thanks should be sent to the client, at the recorded address. This will serve the dual purpose of thanking them for opening the account and for verification of genuineness of address provided by the account holder. Further transactions should not be allowed if the mail is returned. The undelivered envelope should be retained with the KYC papers for further inquiries, if necessary.

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

- The Company will 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, the Company shall obtain senior management approval to continue the business relationship.

- 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.

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

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.

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.

VIII. Risk Management

- Risk Based Approach:

i. 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.

ii. 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 registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries 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 registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

iii. 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:

i. 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.

ii. 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.

iii. 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:

a) To undertake the Money Laundering / Terrorist Financing risk assessments prior to the launch or use of such products, practices, services, technologies; and
b) Adoption of a risk based approach to manage and mitigate the risks

iv. 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 (the links are provided in Para No. XVIII of the KYC PML Policy).

IX. Monitoring of Transactions

All the client accounts are to be monitored at least once every six months and any exceptions need to be reported to the management and compliance department/ Principal Officer.

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. If any transaction appears to be suspicious it is to be reported to the Compliance Department/ Principal Officer immediately.

The Company shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The intermediary 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/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

The registered intermediaries 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.

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 intermediary.

Further, the compliance cell of the Company shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

For identifying the suspicious transactions, the following illustrative questions may be considered:

- Is the customer willing to accept uneconomic terms without apparent reason?
- Is the transaction inconsistent with legitimate business activity?
- Is the transaction inconsistent with the normal pattern of the customer's investment activity?
- Is the transaction inconsistent with the customer's account-opening documents?
- Has the customer requested that the transaction be cleared in a way that is inconsistent with normal practice?
- Is the client financially capable of the transactions he has asked for?

X. Symptoms of Suspicious transactions

An indicative list of suspicious transactions is as follows:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to or insists on dealing only in cash or asks for exemptions from the Company's policies relating to non-acceptance of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs.10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason engages in transactions involving certain types of securities, such as Z group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity.
- The customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

Caution should be exercised if broking/DP accounts have been in-operative for more than 6 months and activity resumes thereafter.

Care should also be taken if the clients make high value payments (Rs. 10 lakhs and above) from bank accounts not declared to us in the KYC forms, or when they make payments through Demand Drafts and not cheques drawn on their declared bank accounts. The details of such transactions should be noted in a separate register.

Caution should be exercised if there any high quantity/value off-market transactions in DP accounts. Caution should also be exercised if large credits in a broking account are advised to be transferred to any broking account with us.

The compliance department shall undertake random checks as to the nature of transactions and whether they are suspicious transactions.

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.

It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

XI. Maintenance of records

- The Securities Contracts Regulation Act, 1956 (SCRA) and SEBI (Stock brokers) Regulations, 1992 provide for maintenance of records for a minimum period of five years. The records and documents as a Depository Participant shall be preserved for a minimum period of eight years in terms of regulation 66(5) of the SEBI (Depositories and Participants) Regulations, 2018.

(i) The following records need to be maintained for stock broking activity:

a) Register of transactions (Sauda book)
b) Client's ledger
c) General Ledger
d) Journals
e) Cash book
f) Bank pass-book
g) Documents register showing full particulars of shares and securities received and delivered and the statement of account and other records relating to receipt and delivery of securities.
h) Member's contract books showing details of all contracts entered into by him with other members of the same exchange or counterfoils or duplicates of memos of confirmation issued to such other members.
i) Counterfoils or duplicates of contract notes issued to clients.
j) Written consent of clients in respect of contracts entered into as principals.
k) Margin deposit book
l) Register of accounts of sub-brokers
m) An agreement with a sub-broker specifying the scope of authority, and responsibilities of the Stock-broker and such Sub-broker;
n) An agreement with the sub-broker and with the client of the sub-broker to establish privity of contract and the client of the sub-broker.

(ii) Records to be maintained for a minimum period of eight years for depository participant business in terms of SEBI (Depositories and Participants) Regulations, 2018:

a) records of all the transactions entered into with a depository and with a beneficial owner;
b) details of securities dematerialized, rematerialized on behalf of beneficial owners with whom it has entered into an agreement;
c) records of instructions received from beneficial owners and statements of account provided to beneficial owners; and
d) records of approval, notice, entry and cancellation of pledge or hypothecation, as the case may be.

(iii) Should there be any suspected drug related or other 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, the Company shall retain the following information for the accounts of their 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

- 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 intermediary has ended or the account has been closed, whichever is later.

- 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 between the client and the intermediary.

- The records are to contain the following information:
    a) the nature of transactions;
    b) the amount of the transaction and the currency in which it was denominated;
    c) the date on which the transaction was conducted; and
    d) the parties to the transaction.

- In the 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.

- Where the registered entity does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.
  Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

XII. Principal Officer

The company has designated the Compliance Officer as the Principal Officer who shall be responsible for implementation and compliance of this policy. His illustrative duties will be as follows:

- Monitoring the implementation of Anti Money Laundering Policy
- Reporting of transactions and sharing of information as required under the law. Making a note of Suspicious Transactions and reporting to Financial Intelligence Unit (FIU-IND).
- Liasoning with law enforcement agencies
- Ensuring submission of periodical reports to the Board of Directors.
- Providing clarifications to staff members of the provisions of the Act, rules, guidelines and the policy of the company.

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.

XIII. 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 —

i. the Managing Director or a Whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
ii. the managing partner if the reporting entity is a partnership firm,
iii. the proprietor if the reporting entity is a proprietorship concern,
iv. the managing trustee if the reporting entity is a trust,
v. 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
vi. 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.

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

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

XIV. Staff awareness and training

Staffs who deal directly with the public are the first point of contact for potential money launderers. Their efforts are therefore vital to the effective functioning of the reporting system for such transactions. Staff should keep themselves abreast of the practices to identify suspicious transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. In short, employees must familiarize themselves with their customers' normal trading activities and usual market practices in order to recognize anomalous behavior. Suspicions concerning the source of assets or the nature of the transaction should not be ignored. It is the active responsibility of every person at the Company to seek to ensure that the Company's facilities are not being misused.

Staff should also not disclose to the customer concerned or to other third persons that the transaction is deemed suspicious or that investigative steps are being taken or that information may be transmitted to the authorities.

The importance of PMLA guidelines and the action required to be taken by the employees in respect of the functions performed by them is being included as a module during induction training or refresher course.

XV. Investors Education

Implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information.

There is, therefore, a need for intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework.

The compliance officer shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

XVI. Hiring Policy

Preference is given to candidates referred by our existing employees, employees of group concerns.

Interview by HR
Interview by head of the department which has requisitioned for filling vacancy.

Employee background checks are conducted using information available on the internet, references provided by candidates, and independently through partnerships with recruitment agencies or third-party verification services.

No candidate is selected who has dubious character or if there is negative information provided by his or her reference.

Using an external search firm is generally discouraged; however, if necessary, we may engage one to explore potential candidates. Regardless, our standard procedure for candidate selection remains unchanged. Additionally, we conduct reference checks in addition to utilizing recruitment agencies.

After the selection, the candidate has to adhere to code of conduct as prescribed by TATA group from time to time.

XVII. Periodicity of Review of PMLA policy:

Necessary amendments / modifications shall be carried out to the Policy as advised by SEBI from time to time. For changes to be made to the Policy on account of regulatory developments, the Compliance Officer shall have the authority to carry out such changes to the Policy.

PMLA policy shall be reviewed at least once in every financial year.

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

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).

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'.

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.

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

The 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.

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 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.

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.

Directions under Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

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 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 WMD Act, 2005.

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 Chief 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, stock exchanges and registered intermediaries shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO, without delay.

d) send a copy of the communication, mentioned in paragraphs (b) and (c) 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 covered all transactions in the accounts, covered under paragraphs (b) and (c) above, carried through or attempted through.

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

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

PART B

Guidelines on Know Your Customer / Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT)

I. Preamble

TATA Securities Limited ("the Company") was issued license to act as a Point of Presence (POP) under Regulation 3 (i) i.e. National Pension System (NPS) – Distribution and servicing for public at large through physical as well as online platforms for National Pension System and other schemes regulated and administered under the provisions of the Pension Fund Regulatory and Development Authority (PFRDA) (Point of Presence) Regulations, 2018 (including amendments thereof).

This Policy is being put in place to comply with the provisions of the PFRDA (Point of Presence) Regulations, 2018 read with PFRDA Circular No. PFRDA/ 2023/ 21/ SUP-POP/04 dated 30th June, 2023 on Guidelines for Operational Activities – to be followed by Point of Presence (PoPs) performing activities of National Pension System (NPS) & PFRDA Circular No. PFRDA/2023/05/REG-POP/02 dated 12th October, 2023 on Guidelines on Know Your Customer/ Anti-Money Laundering/ Combating the Financing of Terrorism (KYC/AML/CFT) issued by the Pension Fund Regulatory and Development Authority.

As per the abovementioned PFRDA Regulations/ Circulars, every entity registered as Point of Presence (PoP) is required to comply with the requirements of Prevention of Money Laundering Act, 2002 as amended from time to time.

II. Definitions

i. "Aadhaar number" as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

ii. "Act/ PML Act/ PMLA" means the Prevention of Money Laundering Act, 2002 as amended from time to time.

iii. "Authentication", means the process as defined under clause (c) of section 2 of the Aadhaar Act.

iv. "Central KYC Records Registry" (CKYCR) means an entity defined under clause (ac) of sub rule (1) of Rule 2 of the PML Rules.

v. "Certified copy" shall mean comparing the copy of officially valid document so produced by the subscriber with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by PFRDA.

vi. “Client” means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting.

vii. “Client Due Diligence” (CDD) shall have the meaning assigned to it under clause (b) of sub-rule (1) of Rule 2 of the PML Rules.

viii. “Designated Director" shall means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV – (Records containing information) of the Act and the Rules.

ix. “Digital KYC” shall means the capturing live photo of the client and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company.

x. “Equivalent e-document” shall means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the client as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

xi. “Financial Group” means a group that consists of a parent company or of any other type of entity exercising control and coordinating functions over the rest of the group, together with branches and/ or subsidiaries that are subject to AML/ CFT policies and procedures at the group level.

xii. “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR.

xiii. “KYC Identifier” shall means the unique number or code assigned to a client by the Central KYC Records Registry.

xiv. “KYC Records” shall have the meaning assigned to it under clause (cd) of sub-rule (1) of Rule 2 of the PML Rules.

xv. “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company as amended from time to time.

xvi. “Offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Unique Identification Authority of India.

xvii. “On-going Due Diligence” means regular monitoring of transactions to ensure that they are consistent with the subscriber’s profile and source of funds.

xviii. "Officially valid document" means the passport, the driving licence,proof of possession of Aadhaar number,the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India or the National Population Register] containing details of name, address and Aadhaar number.

xix. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

xx. "Rules/ PML Rules" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

xxi. "Periodic updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by PFRDA.

xxii. "Principal Officer" shall means an officer nominated by the Company, responsible for furnishing information as per rule 8 of the Rules. Further such officer shall be an officer at the management level.

xxiii. "Reporting entity" has the same meaning assigned to it under clause (wa) of sub section (1) of section 2 of the PML Act.

xxiv. "Suspicious Transaction" shall means a transaction referred to in clause (h), including an attempted transaction, whether or not made in cash, which to a person acting in good faith-
(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to have no economic rationale or bona fide purpose; or
(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation. - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

xxv. "Video Based Customer Identification Process (VCIP)" means an alternative (optional) electronic process of Identification/ KYC in paperless form, carried out by the reporting entities by undertaking seamless, secure, real-time with

geo- tagging, consent based audio-visual interaction with the subscriber to obtain identification information including the necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the subscriber.

xxvi. "Subscriber" shall have the meaning as per clause (t) of sub-section (1) of section 2 of the PFRDA Act. In these guidelines, the phrase Subscriber, Customer and Client has been used interchangeably and shall be considered to have the same meaning.

Words and expressions used and not defined in the policy but defined in the Pension Fund Regulatory and Development Authority Act, 2013, the PML Act, the PML Rules, the Aadhaar Act, Unlawful Activities (Prevention) Act, 1967 shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

III. Objective

The objective of this Policy is to establish an anti-money laundering mechanism and formulate and implement a Client Due Diligence (CDD) Program which will apply to the Company as per provisions of clause (ii) and (iii) sub rule (14) of Rule 9 of the PML Rules. The Company shall have the responsibility for guarding against NPS, NPS Lite, APY or any other pension scheme regulated/ administered by PFRDA being used to launder unlawfully derived funds or to finance terrorist acts. The Company is required to follow Customer Identification Procedures (CIP) while undertaking a transaction at the time of establishing an account-based relationship/ client-based relationship and monitor their transactions on an on-going basis.

IV. Internal policies, procedures, controls, responsibility and compliance arrangement

A. The Company will establish and implement policies, procedures, internal controls and formulate and implement a Client Due Diligence (CDD) Program that effectively serve to prevent and impede Money Laundering (ML) and Terrorist Financing (TF).

B. The senior management of the Company will 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:

(1) Develop a KYC/ AML/ CFT program comprising of policies and procedures, for dealing with KYC, ML and TF reflecting the current statutory and regulatory requirements.
(2) Ensure that the content of these guidelines is understood by all employees, business correspondents, associated Retirement Advisers, PoP Sub-Entity and agents engaged in facilitating distribution of NPS/ APY or any other pension scheme regulated or administrated by PFRDA and develop awareness and vigilance to guard against ML and TF amongst them.

(3) The KYC/ AML/ CFT policy has been approved by the Board of Directors of the Company. The program and processes emanating from the Board approved policy shall be reviewed periodically on the basis of risk exposure and suitable changes (if any) be effected based on experience and to comply with the extant PML Act/ PML Rules/ Regulations/ Guidelines and other applicable norms.
(4) The Board of Directors shall be apprised of the observations, violations, reporting etc., including follow-up action on periodic basis.
(5) Undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of subscriber, business relationship or transaction.
(6) Have in place a system for identifying, monitoring and reporting suspected ML or TF transactions to Financial Intelligence Unit – India (FIU-IND) and the law enforcement authorities in accordance with the guidelines issued by Government of India.

C. Policies and procedures set under KYC/ AML/ CFT program shall cover:

(1) Communication of policies relating to prevention of ML and TF to all level of management and relevant staff that handle subscribers' information (whether in branches or departments) in all the offices of the Company;
(2) The Client Due Diligence Program including policies, controls and procedures, approved by the Board of Directors of the Company to manage and mitigate the risk that have been identified by the Company;
(3) Maintenance of records;
(4) Compliance with relevant statutory and regulatory requirements;
(5) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;
(6) 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 frontline staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of subscribers and other such factors.

D. Responsibility of reporting entities:

The responsibility of a robust KYC/ AML/ CFT program is on the Company. This necessitates that the following steps are to be taken to strengthen the level of control on employees, business correspondents, associated Retirement Advisers, PoP Sub-Entity and agents of the Company:

(1) Standard Operating Procedure/ Guidance note/ Process document covering responsibilities of representatives of the Company must be put in place. A clause to this effect should be suitably included as part of the contract(s) entered with them.

(2) The Company shall initiate appropriate actions against defaulting representative of the Company who expose the Company to KYC/ AML/ CFT related risks on multiple occasions.

(3) The Company is allowed to engage the services of individual like business correspondents or agents for facilitating the distribution of pension schemes, thus the engagement process of such individuals shall be monitored scrupulously in view of set KYC/ AML/ CFT measures.

(4) Financial groups shall be required to implement group-wide programmes against ML/ TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group:

   a. policies and procedures for sharing information required for the purposes of Customer Due Diligence and ML/ TF risk management;
   b. the provision, at group-level compliance, audit, and/or AML/ CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/ CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done). Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and
   c. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(5) The overseas branches of the Company to conduct client due diligence/ AML standard for the subscribers specified by the PFRDA for the pension scheme regulated/ administered by PFRDA. If the host country does not permit implementation of these guidelines, the Company should apply appropriate additional measures to manage the money laundering and terrorist financing risks and inform the same to PFRDA.

E. Certificate of Compliance:
The Company shall submit certificate of compliance as provided in Annexure 1 along with submission of Annual Compliance Certificate i.e., till 31st October of succeeding Financial Year.

V. Appointment of a Designated Director and a Principal Officer

The Company has appointed “Designated Director”, who will ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules.

The Company will appoint “Principal Officer” (PO) at a senior management who will ensure compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules.

The contact details (including mobile number, email ID and business address) of the Designated Director and the Principal Officer shall be submitted within 30 days. Any

changes thereon shall be communicated to PFRDA and FIU-IND within 30 days of its effect.

VI. Recruitment and Training

The Company will ensure that adequate screening mechanism as an integral part of their personnel recruitment/ hiring process shall be put in place.

Further, on-going training programme shall be put in place so that the members/ staff are adequately trained in KYC/ AML/ CFT policy. The focus of the training shall be different for frontline staff, compliance staff, staff dealing with new subscribers. The frontline staff shall be specially trained to handle issues arising from lack of subscriber education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/ AML/ CFT policies of the Company, guideline and related issues shall be ensured.

VII. Internal Control/ Audit

Internal audit/ inspection department of the Company or the external auditor appointed by the Company shall periodically verify compliance with the extant policies, procedures and controls related to money laundering activities on the basis of overall risk assessment. The Company will also upgrade its questionnaire and system from time-to-time in accordance with the extant PML Act and PML Rules. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. The Company shall submit audit notes and compliance to the Audit Committee and in its absence directly to the Board.

VIII. Know Your Customer (KYC) Norms

A. KYC Norms

The Company should make best efforts to determine the true identity of subscriber(s).

The Company shall not allow the opening of or keep any anonymous account or account in fictitious names or whose identity has not been disclosed or cannot be verified. Effective procedures should be put in place to obtain requisite details for proper identification of new/ existing subscriber(s).

The Company shall verify the identity, address and recent photograph in compliance with provision as specified in PML Rules.

At any point of time, where the Company is no longer satisfied about the true identity and the transaction made by the subscriber, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND), if it is satisfied that the transaction meets the criteria specified in sub clause (g) of clause (1) of Rule 2 of the PML Rules and guidelines/ indicators issued by FIU-IND or PFRDA.

The Company may perform KYC process by any of the following methods:

- Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PML Act Or
- Aadhaar based KYC through offline verification Or
- Digital KYC as per PML Rules Or
- Video Based Customer Identification Process (VCIP) as consent based alternate method of establishing the subscriber's identity using an equivalent e-document of any officially valid document (the reporting entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified in Annexure I of PML Rules and the VCIP process for various activities under NPS as has been laid down by PFRDA vide circular no. PFRDA/2020/46/SUP-CRA/18 dated 6th October, 2020 Or
- By using "KYC identifier" allotted to the subscriber by the CKYCR Or
- By "using Digilocker" as prescribed by the PFRDA vide circular no. PFRDA/2021/5/PDES/5 dated 3rd February 2021 Or
- By using certified copy of an 'officially valid document' containing details of the identity and address, recent photograph and such other documents including financial status of the subscribers

  AND

- PAN/Form 60 (wherever applicable) and any other documents as may be required

It is imperative to ensure that the contribution should not be disproportionate to income.

B. Client Due Diligence (CDD)

The Company shall undertake CDD as per the provisions of Rule 9 of PML Rules. Accordingly, the Company shall undertake CDD as follows:

i. Knowing new subscriber
   In case of every new subscriber, necessary client due diligence with valid KYC documents of the subscriber shall be done at the time of commencement of account-based relationship/ client-based relationship. Such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients.

ii. Knowing existing subscribers
   - The AML/ CFT requirements are applicable for all the existing subscribers. Hence, necessary CDD with KYC (as per extant PML Rules) shall be done for the existing subscribers from time-to-time basis the adequacy of the data previously obtained. Further, periodic updation of KYC of NPS account shall be done as follows:
     a. In case of NPS Tier II accounts (excluding Tier II Tax Saver Scheme) - Every 3 years.
     b. In case of Tier II account, where subscriber is Politically Exposed Person (PEP) – Every 2 years.
     c. At the time of exit from NPS Tier I account.

d. Whenever there is upward revision in the risk profile of the subscriber.
e. As and when there are revision or changes in PML Act / PML Rules.

- Where the risks of money laundering or terrorist financing are higher, the Company should be required to conduct enhanced due diligence (EDD) measures, consistent with the risks identified.
- Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the Client Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file an Suspicious Transaction Report (STR) with FIU-IND.

iii. Ongoing Due Diligence

Besides verification of identity of the subscriber at the time of opening of pension account/ initial contribution, risk assessment and ongoing due diligence should also be carried out at times when additional/ subsequent contributions are made.

Any change which is inconsistent with the normal and expected activity of the subscriber should attract the attention of the reporting entities for further ongoing due diligence processes and action as considered necessary.

The Company shall identify the source of contribution and ensure that the contribution is being made through the subscriber's source of funds.

Verification at the time of exit (superannuation /premature exit / death etc.)

a. No payments should be made to third parties on attainment of superannuation except payments to nominee(s)/ legal heir(s) in case of death.
b. Necessary due diligence of the subscriber(s) / nominee(s) / legal heir(s) should be carried out before making the pay-outs/settling claims.

Notwithstanding the above, the Company is required to ensure that no vulnerable cases go undetected, especially, where there is suspicion of money-laundering or terrorist financing, or where there are factors to indicate a higher risk, necessary due diligence will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

IX. Risk Assessment and Risk Categorization

A. While assessing the subscriber`s risk profile under pensions schemes regulated /administered by PFRDA, the company may inter-alia take into account the following:
   - Whether contributions are mandatory contribution viz Employees of central /state government/ autonomous bodies/ public sector undertakings covered under NPS (These accounts would generally involve lower risk)

- Whether contributions are voluntary and low-contribution: APY being fixed and low contribution pension scheme and NPS Lite being low contribution pension scheme (These accounts generally involve lower risk)
- Contributions towards NPS Tier I account on a voluntary basis (These accounts generally involve moderate risk)
- Voluntary contributions towards NPS Tier II account, which is a withdrawable account (These accounts involve generally higher risk in comparison to other categories)

B. Notwithstanding anything contained in IX.A above, while assessing the subscriber's risk profile, the Company will consider the following factors:
   - Nature of account (For e.g. - NPS Tier I, NPS Tier II, NPS Tier II Tax Saver Scheme, NPS Lite, APY and any other scheme regulated/administered by PFRDA)
   - Source of contribution
   - Mode of contribution (Cash /Online /Cheque /DD/ Card/ employers bank account etc.)
   - Regularity in the flow of contribution (For e.g. – Contributions under employer and employee relationship)
   - Withdrawals under Tier I and Tier II account
   - Residence status of subscriber (For e.g. – Subscribers residing in jurisdiction with higher national risk assessment)
   - Politically Exposed Person
   - Contributions made by the subscriber vis-à-vis the declared income/ income range.

   Additional factors will be included going forward using judgement and experience as the above list is indicative and not exhaustive.

C. The Company have to carry out ML and TF Risk Assessment exercise as provided in sub rule (13) of Rule 9 of PML Rules based on risk exposure to identify, assess, document and take effective measures to mitigate its ML and TF risk for subscribers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. While assessing the ML/ TF risk, the Company is required to take cognizance of the overall sector specific and country specific vulnerabilities, if any, that the Government of India/ PFRDA may share with reporting entities from time to time. Further, the internal risk assessment carried out by the Company should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

D. The documented risk assessment shall be updated from time to time. The company 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. It shall be made available to competent authorities and law-enforcement agencies, as and when required.

E. Risk Categorization:

- Risk categorization shall be undertaken based on parameters detailed at clause A and B besides others like subscriber's identity, nature of employment, high value deposits in Tier II account/ in Tier I account near superannuation, unusual withdrawals in Tier II account etc. While considering subscriber's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. The Company shall ensure enhanced due diligence (EDD) for NPS Tier II account (except accounts under NPS Tier II Tax Saver Scheme)

- For the purpose of risk categorization, individuals whose identities and source of income can be easily identified and transactions in whose pension accounts by and large conform to the known profile may be categorized as low-risk. For low-risk subscribers the PRAN account may require only the basic requirements like verifying the identity, current address, annual income and sources of the fund of the subscriber are to be met. Notwithstanding the above, in case of continuing relationship, if the situation warrants, as for examples if the subscriber's profile is inconsistent with the investment through subsequent contributions, a re-look on subscribers profile is to be carried out.

- For the high-risk profiles, like for subscribers who are non - residents, high net worth individuals, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC procedures should ensure higher verification and counter checks.

F. Risk assessment for New Business Practices/ Developments:

The Company shall pay special attention to money laundering threats that may arise from:

a) New business practices including new delivery mechanisms
b) Use of new or developing technologies for the pension schemes regulated/ administered by the PFRDA.

The Company shall undertake the above risk assessment exercise, prior to the use of such practices and technologies and shall take appropriate measures to manage and mitigate the risks.

X. Simplified Due Diligence (SDD)

Simplified measures as provided under clause (d) of sub-rule (1) of Rule 2 of PML Rules are to be applied by the reporting entities in case of accounts opened under APY where the account is classified as Low Risk.

However, Simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high-risk scenarios apply, based on the Risk Assessment/categorization policy of the reporting

entities. The list of simplified due diligence documents are specified in clause (d) of sub- rule (1) of Rule 2 of the PML Rules.

XI. Enhanced Due Diligence (EDD)

Enhanced Due Diligence as mentioned in Section 12AA of PML Act shall be conducted for high-risk categories of subscribers.

The Company should examine, as far as reasonably possible, unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, companies should be required to conduct enhanced due diligence measures, consistent with the risks identified.

The Company shall

- Verify the identity of the subscriber preferably using Aadhaar subject to the consent of subscriber or;
- Verify the subscriber through other modes/ methods of KYC as specified through circulars / guidelines issued by the Authority from time to time.

The Company shall examine the ownership and financial position, including subscriber's source of funds commensurate with the assessed risk of subscriber and his/ her profile.

XII. Sharing KYC information with Central KYC Registry (CKYCR)

Government of India has notified the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

The Company is required to perform the CKYCR related functions in the manner as prescribed under the PML Rules. For the purpose of performing such functions the Company is required to get registered with CERSAI. Presently, under the NPS architecture the Companies registered under regulation 3(1)(i) and Regulation 3(1)(ii) of Pension Fund Regulatory and Development Authority (Point of Presence) Regulations, 2018 shall register themselves with CERSAI. Further, the Company already registered with CERSAI under another financial sector regulator is not required to register themselves with CERSAI again, and may use such registration with CERSAI as the Company under PFRDA as well.

Where a subscriber submits a "KYC identifier" for KYC, the Company shall retrieve the KYC records from CKYCR. In such case, the subscriber shall not submit the KYC records unless there is a change in the KYC information required by the Company as per Rule 9(1C) of PML Rules.

If the KYC identifier is not submitted by the subscriber, the Company shall search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the subscriber, if available.

If the KYC identifier is not submitted by the subscriber or not available in the CKYCR portal, the Company shall capture the KYC information in the manner as prescribed under the PML Rules and as per the KYC Template stipulated for Individuals. The KYC template for 'individuals' and the 'Central KYC Registry Operating Guidelines 2016' for uploading KYC records on CKYCR finalised by CERSAI are available at www.ckycindia.in

The Company shall file the electronic copy of the subscriber's KYC records with CKYCR within 10 days after the commencement of account-based relationship with a subscriber as per the guidelines/ instructions/ circulars by PFRDA from time to time.

Once "KYC Identifier" is generated/ allotted by CKYCR, the Company shall ensure that the same is communicated immediately to the respective subscriber in a confidential manner, mentioning its advantage/ use to the subscriber.

The following details need to be uploaded on CKYCR if Verification/ Authentication is being done using Aadhaar:

I. For online Authentication,
   a) The redacted Aadhar Number (Last four digits)
   b) Demographic details
   c) The fact that Authentication was done

II. For offline Verification
   a) KYC data
   b) Redacted Aadhaar number (Last four digits)

At the time of periodic updation, it is to be ensured that all existing KYC records of subscriber are incrementally uploaded as per the extant CDD standards. The Company shall upload the updated KYC data pertaining to active pension accounts against which "KYC identifier" are yet to be allotted/ generated by the CKYCR.

The Company shall not use the KYC records of the subscriber obtained from Central KYC Records registry for purposes other than verifying the identity or address of the subscriber and should not transfer KYC records or any information contained therein to any third party as per Rule 9(1F) of PML rules unless authorised to do so by the subscriber or PFRDA or by the Director (FIU- IND). The Company shall ensure that in case of accounts that have been opened prior to operationalisation of CKYCR, the KYC records are updated in the CKYCR during periodic updation and that the subscriber's accounts are migrated to current Customer Due Diligence Standards (CDD)

The Company shall submit the MIS related to the CKYC data upload/ download etc. to PFRDA as stipulated from time to time.

XIII. Reliance on third party KYC

For the purposes of KYC norms under clause 8, while the Company is ultimately responsible for subscriber due diligence and undertaking enhanced due diligence

measures, as applicable, the Company may rely on a KYC done by a third party subject to the conditions specified under sub-rule (2) of rule (9) of the PML Rules.

The Company can utlise the SEBI KRA for KYC in accordance with PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019.

The ultimate responsibility for relying on third party KYC is with the REs.

XIV. Pension accounts of Politically Exposed Persons (PEPs)

It is emphasized that proposals of Politically Exposed Persons (PEPs) in particular requires examination by senior management of the Company.

The Company is directed to lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are family members, close relatives/ associates of PEPs. These measures are also to be applied to pension accounts of which a PEP is the beneficiary/ nominee.

If the on-going risk management procedures indicate that the subscriber or beneficiary is found to be PEP or subsequently becomes PEP, the senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

The Company to take reasonable measures to determine whether the beneficiaries of a pension account are PEPs at the time of the exit, and should ensure the internal controls are in place. The Company that processes exit request should apply risk-based monitoring of such withdrawal to determine if the recipient of the funds is a PEP.

The Company shall undertake reasonable measures to establish the source of wealth and the source of funds of customers identified as PEPs.

XV. Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated 2nd February 2021 detailing the procedure for the implementation of Section 51A of the UAPA.

The Company should not open pension account of a subscriber whose identity matches with any person in the UN sanction list and those reported to have links with terrorists or terrorist organizations.

The Company shall periodically check MHA website for updated list of banned individuals.

The Company shall maintain an updated list of designated individuals in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals are holding any pension accounts. An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list and UNSC 1988 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1988/materials.

By virtue of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), the Central Government is empowered to freeze, seize or attach funds of and/ or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. [The list is accessible at website http://www.mha.gov.in]. To implement the said section an order reference F. No. 14014/01/2019/CFT dated 2nd February, 2021 has been issued by the Government of India. The salient aspects of the said order with reference to insurance sector would also be applicable to NPS / NPS Lite / APY or any other scheme regulated or administered by PFRDA.

The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

XVI. Prospects residing in the jurisdiction of countries identified as deficient in AML/ CFT regime

The Company is required to:

- Specifically apply enhance due diligence (EDD) measures, proportionate to the risks, to business relationships and transactions with individual from countries for which this is called for by the FATF.
- Pay special attention to unusual contributions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will, as far as possible, have to be examined and written findings have to be maintained for assisting competent authorities.
- Agents / intermediaries / employees to be appropriately informed to ensure compliance with this stipulation.
- Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendation.
- Take similar measures on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

XVII. Reporting Obligations

The Company shall furnish to the Director, Financial Intelligence Unit- India (FIU-IND), information referred to in Rule 3 of the PML Rules in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified in September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU- IND shall have powers to issue guidelines to the reporting entities for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR)/ Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by the Company which are yet to install/ adopt suitable technological tools for extracting CTR/ STR from their live transaction data. The Principal Officers of those Companies, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

Red Flag Indicators issued by FIU-IND and PFRDA also be taken in account for Suspicious Transaction, wherever necessary. Indicative Red Flag Indicators (RFis) for the intermediaries registered with PFRDA is as per Annexure 2.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the subscriber at any level. Confidentiality requirement does not inhibit information sharing among entities in the group.

Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the subscribers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

The Company shall leverage the broadest number of data points/ records available with them in implementing alert generation systems to assist in identifying and reporting suspicious activities.

The Company should not enter into arrangement with any unregulated entity which may have the effect of directly or indirectly impairing any reporting obligations of the reporting entities.

XVIII. Record Keeping

In view of Rule 5 of the PML rules, the Company, its Designated Director, Principal Officer, employees are required to maintain the information/ records of types of all transactions [as mentioned under Rules 3 and 4 of PML Rules 2005] as well as those

relating to the verification of identity of subscribers for a period of five years. The records referred to in the said Rule 3 shall be maintained for a period of five years from the date of transaction. Records pertaining to all other transactions, (for which reporting entities are obliged to maintain records under other applicable Legislations/ Regulations/ Rules) the Company is directed to retain records as provided in the said Legislation/ Regulations/ Rules but not less than for a period of five years from the date of end of the business relationship with the subscriber.

Records can be maintained in electronic form and/ or physical form. In cases where services offered by a third-party service providers are utilized,

- The Company shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data
- The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored and recorded.
- The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.
- It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.

The Company should implement specific procedures for retaining internal records of transactions, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. The Company should retain the records of those accounts, which have been settled by claim, for a period of at least five years after that settlement.

In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, the Company is required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.

In case of subscriber identification, data obtained through the subscriber due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

XIX. Monitoring of Transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the KYC/ AML/ CFT procedures. This is possible only if the Company have an understanding of the normal activity of the subscriber so that it can identify deviations in transactions/ activities.

The Company shall pay special attention to all complex large transactions/ patterns which appear to have no economic purpose. The Company may specify internal threshold limits for each class of subscriber 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 PFRDA/ FIU-IND/ 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.

The Principal Officer of the Company shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU- IND.

Further, the compliance cell of reporting entities shall randomly examine a sample of transactions undertaken by subscribers to comment on their nature i.e., whether they are in nature of suspicious transactions or not.

Notwithstanding anything contained in these guidelines, in case of any issue with respect to interpretation of any provision of these guidelines, the provisions/ directives of the FIU India, the PML Act / the Aadhaar Act / Income Tax Act and their rules as amended from time to time, will prevail.

The Company is also advised to refer to the extant relevant directives, rules, laws and provisions mentioned therein on a regular basis to broadly understand, apply, update their KYC/ AML /CFT programme and implement the provisions of this guideline.

XX. Review of Policy

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.The Policy would be available on the Company’s registered office and all the Branches of the Company.

Annexure 1

Certificate of Compliance with respect to KYC/AML/CFT

Name of Reporting Entity:
Financial Year:

We do hereby submit that……. (name of the reporting entity) has fully complied with all the norms laid down by PFRDA and with the extant PML Act I PML Rules.

Designated Director (Name and Signature along with the stamp of the entity)
(* to be submitted along with submission of Annual Compliance Certificate)

Annexure 2

Annexure A - Indicative Red Flag Indicators (RFis) for the intermediaries registered with PFRDA

Alert Source	Alert Indicator	Intermediary to Generate Alerts	Indicative Rule/ Scenario
Customer Verification	**CV8 – Name of subscriber found in the watch list**	Point of Presence (PoP)	Name of subscriber(s) found in the watch list such as Ministry of Home Affairs (MHA) list/ Unlawful Activities (Prevention) Act (UAPA)/ Weapons of Mass Destruction and Delivery System Act (WMDA)/ United Nations Security Council Resolution (UNSCR) / Office of Foreign Assets Control (OFAC) and any other lists.
	CV9 - Non-cooperation by the subscriber		Non-cooperation of the subscriber in furnishing information to examine the Reporting Entities to examine the ownership and financial position.
	CV10 – Inconsistent activity of the subscribers having high risk profiles		Any change which is inconsistent with the normal and expected activity of the subscribers having high-risk profiles, like for subscribers who are high net worth individuals, non-residents, Politically Exposed Persons (PEPs), and those with dubious reputation as per available public information.
Transaction Monitoring	**TM5 - Use of Demand Drafts for subscription**	Point of Presence (PoP)	Demand drafts of value below Rs. 50,000.00 have been used for investing in a rolling period of 1 year and the cumulative amount of such subscriptions is Rs. 2 lac and above.
	TM6- Unusual patterns of transactions		Unusual patterns of transactions, which have no apparent economic or lawful purpose where the risks of money laundering or terrorist financing are higher.
	TM7- Requests for withdrawal to a different bank		Subscribers made subscription from a given bank mandate and made a withdrawal request with a different bank mandate.

	mandate.		
	TM8- Change in bank mandate during a rolling 12-month period	**Point of Presence (PoP)**	Changes to bank mandate are executed by individual investors (including HUF) involving more than three different bank accounts (account numbers are different). These changes are over and above registered bank accounts.
	TM9- Use of different Accounts by subscriber(s) alternatively		Subscriber(s) making subscription via more than five bank accounts during last one year
	TM10- Contribution disproportionate to the Income of the subscriber		Contribution of the subscriber during a financial year is disproportionate to the annual income specified by that subscriber in the KYC form. ** The reporting entities may specify internal threshold limits for each class of subscriber accounts.*
	TM 11 - high value subscription		Subscriber made high value subscription near his/ her superannuation.
	TM 12 – Abuse the provisions of PAN Exemption		Transactions made by subscriber(s) through abusing the provisions of PAN Exemption in order to avoid submitting PAN at the time of subscription(s).