Max Life PFM Pension Fund Management Limited

Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) Policy and Program

Date: April 25.2023
Version: 1.0

TABLE OF CONTENTS

1. Principles of the Company's AML/CFT Policy

- The Prevention of Money Laundering Act, 2002 (PMLA), brought into force with effect from 1st July 2005, is applicable to all financial institutions. Giving reference of this Act, PFRDA has released guidelines on Know Your Customer / Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT) dated 23rd January, 2023 ("Guidelines") in this regard for entities registered as Point of Presence (PoP) under the PFRDA (Point of Presence) Regulations, 2018. In these Guidelines, PFRDA has mandated that each registered entity should have an AML/CFT program ("Program"). This Program would serve the purpose of discharging the PoPs statutory responsibility including the detection and reporting of possible attempts of money laundering or financing of terrorism. The Program includes procedures defined by the management/various functions in respective standard operating procedures (SOPs).

- To adhere to the Guidelines, Max Life Pension Fund Management Limited ("Company", "Max Life PFM") has prepared an anti-money laundering/counter financing of terrorism policy ("Policy") and Program and mandates strict compliance with the same.

- Max Life PFM requires its employees, business correspondents, associated retirement advisers, PoP Sub-entity agents, and intermediaries to adhere to all the applicable laws, rules and regulations generally in relation to AML/CFT norms and also the specific requirements mentioned in this Policy. The Company has a zero tolerance for any violations to the requirements detailed in this Policy**.** Any exception should be brought to the immediate attention of the Company's Principal Officer. In case of violations to this Policy, Max Life PFM reserves the right to take appropriate management measures (at its sole and absolute discretion) as defined in its disciplinary action policies, including the termination of its relationship with the concerned.

- The Company shall undertake procedural checks to ensure that it has knowledge of the basis on which Clients propose to purchase the policies. A strict application of these procedures and controls is essential for all relevant transactions of the Company. The Program is set out in detail in the following sections to ensure that comprehensive procedures are laid down, clearly communicated to all the concerned persons and strictly followed. Further, the Program requires the institution of effective controls to detect procedural lapses, if any, and ensure timely remediation. The standards on procedures and controls are embedded in the SOPs, which have to be created by relevant functions.

- Function heads have the primary responsibility for implementing this Policy within their areas of responsibility. Compliance function has the responsibility of making all the filings with the PFRDA and FIU-India within the specified timelines.

- The management, in furtherance of responsibilities of the Designated Director, as outlined in section 4 herein, has the primary responsibility of:

    - Developing the Program comprising policies and procedures, for dealing with money laundering (ML) and terror funding (TF) in compliance with current statutory and regulatory requirements

- Undertaking all actions as specified under the Guidelines and any subsequent amendments or clarifications thereof to implement the provisions of Act and Rules, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).
- Ensuring compliance with all relevant sections as specified under the FIU-India's guidance document, as applicable ("FIU-India") as amended from time to time. In case of any issue with respect to interpretation of any provision of the Guidelines, the provisions/ directives of FIU-India, the Act/Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act/Income Tax Act and their rules as amended from time to time, will prevail.
- Providing all assistance to the Central Government in order to implement the provisions of the Unlawful Activities (Prevention) Act, 1967, ("**UAPA**") as detailed in Section 14 of this Policy.

- Training is an essential part of the Program to ensure awareness of the requirements and vigilance to guard against ML and TF by all concerned persons. Company shall ensure that the content of the Guidelines is understood by all staff members.

- The Program shall be reviewed periodically on the basis of risk exposure and suitable changes (if any) shall be affected based on experience and to comply with the extant law.

- The Policy is a Board approved policy. Deviations to this Policy are to be reported to the Risk Committee of the Board.

- Any amendment in applicable regulatory requirements is required to be notified to the Risk Committee of the Board.

- Administration of the Policy shall be done basis the function-wise SOPs on various aspects including procedures for Client identification, record-keeping, acceptance and processing of applications.

- The Policy shall come into effect on 1st April, 2023.

- A list of definitions and abbreviations used in the Policy are set out in Annexure I.

2. Regulatory requirements for AML/CFT

- PFRDA has been authorized, by virtue of the Rules, to *inter alia*:

  - Lay down "procedure and manner" for maintenance of information in respect of transactions with Client as specified in rule 3 of the Rules
  - Prescribe "form and interval" for maintaining such information by the company
  - Prescribe any document to verify the identity and address of the clients of the company
  - Prescribe a mechanism for reporting obligations

- Following steps will be taken to strengthen the level of control on the intermediaries/representative engaged by the Company:

- Putting in place the list of rules and regulations covering performance of intermediaries /representative of the Company. A clause shall be added making KYC norms mandatory as a part of the contracts.
- Initiating appropriate actions against defaulting intermediaries /representative who expose the Company to AML/CFT related risks on multiple occasions.
- Monitoring the selection process of intermediaries /representative of Company scrupulously, in view of AML/CFT measures.

3. Key elements of the Program

Policy and procedures set under Program shall cover:

- Communication of Policy to all level of management and relevant staff that handle Client's information (whether in branches or departments) in all the offices of the Company;
- The Client due diligence (CDD) program including policies, controls and procedures, as approved by the senior management, to enable the Company to manage and mitigate the risk that have been identified either by the Company or through national risk assessment;
- Maintenance of records;
- Compliance with relevant statutory and regulatory requirements;
- Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;
- Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF.

The requirements under this Policy for ensuring compliance with the key elements of the Company's Program are described below.

4. Appointment of a Principal Officer and Designated Director

Appointment of a Principal Officer

- As per PFRDA's requirements, the Company has designated the CEO as its Principal Officer and has communicated his/her contact details with mobile number and email id to both PFRDA and FIU-India within 30 days from the date of issuance of these Guidelines and any changes thereon shall be communicated to PFRDA and FIU-India within 30 days of its effect.

- The Principal Officer shall ensure compliance with the obligations imposed under chapter IV of the Act and the Rules.

Appointment of a Designated Director

- The Company has designated the CEO as its Designated Director and has communicated his contact details with mobile number and email id to both PFRDA and FIU-India within 30 days from the date of issuance of these Guidelines and any changes thereon shall be communicated to PFRDA and FIU India within 30 days of its effect.

- The responsibility of the Designated Director will be to supervise the Program and ensure overall compliance with the obligations imposed under the Guidelines, the Act and the Rules.

5. Recruitment & Training

Adequate screening mechanism as an integral part of personnel recruitment/hiring process is in place.

On-going training program is in place so that the members / staff are adequately trained in Policy. The focus of the training is different for frontline staff, compliance staff, staff dealing with new Clients and claims. The front line staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in Policy, guideline and related issues shall be ensured.

6. Internal Control/Audit

- The Company's internal audit department shall verify on a regular basis that compliance with Policy is adhered to.

- 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 internal audit department shall upgrade its questionnaire and system from time to time.

- The internal audit department shall report any exceptions to the Audit Committee. The Company will submit the audit notes and compliance to the Audit Committee and in its absence directly to the Board or equivalent authority of the Company.

- The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

- Internal audit 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.

7. Know Your Customer (KYC) Guidelines & KYC periodicity

The Company shall undertake procedural checks to ensure that (1) the Company on best efforts basis determines the true identity of the Clients, their interest/s and the origin of the funding of their policy and (2) Special care is exercised to ensure that the contracts are not under anonymous or fictitious names. A strict application of these requirements is essential for all relevant transactions of the Company**.** Effective procedures shall be put in place to obtain requisite details for proper identification of new/existing Client(s).

Given the criticality of the matter, the requirements are set out in detail below.

7.1 KYC Norms

7.1.1 Company shall not allow the opening of or keep any anonymous account or account in fictitious names or persons whose identity has not been disclosed or cannot be verified.

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

7.1.2.1 Aadhaar based KYC through online authentication subject to notification by the Government under section 11A of Act; Or

7.1.2.2 Aadhaar based KYC through offline verification; Or

7.1.2.3 Digital KYC as per Rules; Or

7.1.2.4 Video Based Customer Identification Process (VCIP) as consent based alternate method of establishing the Client's identity using an equivalent e-document of any officially valid document (the Company will 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 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

7.1.2.5 By using "KYC identifier" allotted to the Client by the CKYCR; Or

7.1.2.6 By "using Digilocker" as prescribed by the PFRDA vide circular no. PFRDA/2021/5/PDES/5 dated 3rd February 2021; Or

7.1.2.7 By using certified copy of an 'officially valid document' (duly certified by an authorized person of the Company after checking the original) containing details of the identity and address, recent photograph and such other documents including financial status of the Client.

AND

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

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

7.2 Client Due Diligence (CDD)

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

7.2.1 Knowing new Client

In case of every new Client (including the non-face-to-face Client), necessary CDD with valid KYC documents of the Client will be done at the time of commencement

of account-based relationship/ client-based relationship which will include identifying Clients, verifying their identity, obtaining information on the purpose and intended nature of the business.

7.2.2 Knowing existing Clients

7.2.2.1 Necessary CDD with KYC (as per extant PML Rules) shall be done for the existing Clients 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 the Client is 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 Client.
e. As and when there are revision or changes in Act / Rules.

7.2.2.2 Where the risks of money laundering or terrorist financing are higher, the Company will conduct enhanced due diligence (EDD) measures, consistent with the risks identified.

7.2.3 Ongoing Due Diligence

Besides verification of identity of the Client at the time of opening of pension account / initial contribution, risk assessment and ongoing due diligence will be carried out (if so required) at times when additional/ subsequent contributions are made.

Any change which is inconsistent with the normal and expected activity of the Client should attract the attention of the Company for further ongoing due diligence processes and action as considered necessary. Above mentioned KYC and risk assessment activities shall be carried out as per the applicable AML SOPs.

7.2.3.1 The Company shall identify the source of contribution and ensure that the contribution is being done through the Client's source of funds.

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

a. No payments will 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 Client(s) / nominee(s) / legal heir(s) will be carried out before making the pay-outs/settling claims.

7.2.3.3 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-India, if necessary.

8. Risk Assessment/Categorization

8.1 While assessing the Client`s risk profile under pensions schemes regulated / administered by PFRDA, the Company shall take into account the following:

8.1.1 Low risk -

a. Whether contributions are mandatory contribution viz employees of central / state government / autonomous bodies / public sector undertakings covered under NPS.

b. Whether contributions are voluntary and low-contribution: APY being fixed and low contribution pension scheme and NPS Lite being low contribution pension scheme.

8.1.2 Moderate risk - Contributions towards NPS Tier I account on a voluntary basis.

8.1.3 High risk - Voluntary contributions towards NPS Tier II account, which is a withdrawable account.

8.2 Notwithstanding anything contained in 8.1 above, while assessing the Client's risk profile, the Company will consider the following factors (indicative and not exhaustive).The Company may consider additional factors using own judgement and past experience.:

8.2.1 Nature of account (For eg - NPS Tier I, NPS Tier II, NPS Tier II Tax Saver Scheme, NPS Lite, APY and any other scheme regulated/administered by PFRDA)

8.2.2 Source of contribution

8.2.3 Mode of contribution (Cash / Online / Cheque / DD/ Card/ employers bank account etc)

8.2.4 Regularity in the flow of contribution (For eg – Contributions under employer and employee relationship)

8.2.5 Withdrawals under Tier I and Tier II account

8.2.6 Residence status of Client (For eg – Client residing in jurisdiction with higher national risk assessment)

8.2.7 Politically Exposed Person

8.2.8 Contributions made by the Client vis-à-vis the declared income/ income range

8.3 The Company shall carry out ML and TF risk assessment exercise periodically based on risk exposure to identify, assess, document and take effective measures to mitigate its ML and TF risks for Clients or geographic areas, products, services, nature and volume of transactions or delivery channels etc. While assessing the ML and 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.

8.4 The risk assessment shall be documented and updated from time to time and it shall be made available to competent authorities and law- enforcement agencies, as and when required. Basis the key element of the Program as detailed above, 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. Exceptions, if any, on the key elements towards risk assessment shall be discussed by the respective function heads with Chief Risk Officer (CRO) and shall be tabled at the relevant management meeting.

8.5 ln the context of the very large base of Clients and the significant differences in the extent of risk posed by them, as part of the risk assessment, the Company shall at a minimum, classify the Clients into high risk and low risk, based on the individual's profile, to decide upon the extent of due diligence.

8.6 Risk Categorization:

8.6.1 Risk categorization shall be undertaken based on parameters such as Client'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 Client's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. Company will perform enhanced due diligence (EDD) for NPS Tier II account (except accounts under NPS Tier II Tax Saver Scheme).

8.6.2 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 Permanent Retirement Account Number (PRAN) account may require only the basic requirements like verifying the identity, current address, annual income and sources of fund of the Client are to be met. Notwithstanding the above, in case of continuing relationship, if the situation warrants, as for examples if the Clients profile is inconsistent with the investment through subsequent contributions, a re-look on Clients profile is to be carried out.

8.6.3 For the high-risk profiles, like for Clients 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.

9. Simplified & Enhanced Due Diligence

9.1 Simplified due diligence

9.1.1 Simplified measures are to be applied by the Company in case of accounts opened under APY where the account is classified as low risk. The list of simplified due diligence documents is specified in respective SOP.

However, simplified CDD 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 Company.

9.2 Enhanced Due Diligence (EDD)

9.2.1 Enhanced due diligence as mentioned in Section 12AA of Act shall be conducted for high-risk categories of Clients.

9.2.2. The Company will 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, the Company will be required to conduct enhanced due diligence measures, consistent with the risks identified. As mentioned under the SOP, the following are some of the reasonable measures, that Company shall undertake in carrying out enhanced due diligence, verify:

9.2.2.1. the identity of the Client preferably using Aadhaar subject to the consent of Client or;

9.2.2.2. the subscriber through other modes/ methods of KYC as specified through circulars / guidelines issued by the Authority from time to time.

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

10. Sharing KYC information with Central KYC Registry

10.1 Where a Client submits a "KYC identifier" for KYC, the Company shall retrieve the KYC records from CKYCR. In such case, the Client 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 Rules.

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

10.3 If the KYC identifier is not submitted by the Client or not available in the CKYCR portal, the Company shall capture the KYC information in the manner as prescribed under the 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

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

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

10.6 The following details need to be uploaded on CKYCR if verification / authentication is being done using Aadhaar:

10.6.1 For online authentication,

The redacted Aadhaar number (Last four digits), demographic details; and the fact that authentication was done

10.6.2 For offline verification

KYC data and the redacted Aadhaar number (Last four digits)

10.7 At the time of periodic updation, it is to be ensured that all existing KYC records of Client 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.

10.8 The Company shall not use the KYC records of the Client obtained from Central KYC Records registry for purposes other than verifying the identity or address of the Client and should not transfer KYC records or any information contained therein to any third party unless authorised to do so by the Client or PFRDA or by the Director (FIU-India). 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 Client CDD.

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

11. Reliance on third party KYC:

11.1 For the purposes of KYC norms, while the Company is ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable, the Company may rely on a KYC done by a third party subject to the following conditions.

a. The Company immediately obtains necessary information of such CDD carried out by the third party.
b. Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements shall be made available from the third party upon request without delay.
c. The Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with CDD and record-keeping requirements in line with the requirements and obligations under the Act.
d. The third party is not based in a country or jurisdiction assessed as high risk.
e. Where the Company relies upon third party that is part of the same financial group, they should obtain KYC documents or the information of the CDD within 15 days.

11.2 The Company may utilise the SEBI KYC registration agency KRA for KYC in accordance with PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019

12. Contracts with Politically Exposed Persons (PEPs)

12.1. Company, basis the on-going risk management procedures, shall identify and apply enhanced due diligence measures to PEPs, Clients who are close relatives of PEPs. These measures shall also to be applied to insurance contracts of which a PEP is the ultimate Beneficial Owner.

12.2. Senior Management not below Compliance officer /Chief Risk Officer level will examine proposals of PEPs in particular. Company should lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs. These measures will also be applied to pension accounts of which a PEP is the beneficiary / nominee.

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

12.4. The Company shall take reasonable measures to determine whether the beneficiaries of a pension account are PEPs at the time of the exit, and will ensure the internal controls as per the SOP are in place. The Company while processing exit request will apply risk-based monitoring of such withdrawal to determine if the recipient of the funds is a PEP.

13. Watch List Screening / Implementation of Section 51A of UAPA

13.1. No pension account will be opened by the Company of a Client whose identity matches with any person in the UN sanction list or with banned entities and those reported to have links with banned entities or terrorist organizations. The Company will periodically check MHA website for updated list of banned individuals.

13.2. In case of any record found to be matching with any individual or entities that are suspected to be engaged in terrorism, the procedure for informing / seizing / freezing / unfreezing of the account is to be followed as prescribed under the section 51A of the UAPA.

13.3. 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.

13.4. 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.

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

The Company shall:

14.1. Conduct enhanced due diligence before commencing account-based relationship with individuals residing in the jurisdiction of countries identified by FATF as having deficiencies in their AML/CFT regime.

14.2. 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.

14.3. Agents / intermediaries / employees to be appropriately informed to ensure compliance with this stipulation.

14.4. Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations.

14.5. 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).

15. Reporting Obligations

a Company shall furnish to the Director, Financial Intelligence Unit- India (FIU-India), information referred to in Rule 3 of the Rules vide the procedure outlined in Rule 7 thereof.

b The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-India and report generation utility (RGU) and report validation utility (RGU) developed to assist the Company in the preparation of prescribed reports shall be adhered to.

c While furnishing information to the Director, FIU-India, 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.

d The Company will not put any restriction on operations in the accounts where an STR has been filed and will keep the fact of furnishing of STR strictly confidential. It will be ensured that there is no tipping off to the Client at any level.

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

f 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.

g 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 Company.

h The Company shall have in place a system for identifying, monitoring and reporting suspected ML and TF transactions as mentioned in the Master Guidelines, for furnishing information about such transactions to FIU-India and the law enforcement authorities (if so required).

16. Record Keeping

a In view of Rule 5 of the PML rules, the Company, its Designated Director, Principal Officer, employees shall maintain the information/records of types of transactions as mentioned under Rule 3 and 4 of Rules as well as those relating to the verification of identity of Client for a period of five years. The records referred to in the said Rule 3 will also be maintained for a period of five years from the date of transaction. Records pertaining to all other transactions, for which the Company is required to maintain records under other applicable legislations/regulations/rules, it shall 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 Client.

b 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:

i 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.

ii 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.

iii The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

iv The provisions under the relevant and extant data protection statutes are duly complied with.

c Records shall be maintained in the manner that facilitate ease of complying information requests. 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 will retain the records of those accounts, which have been settled by claim, for a period of at least five years after that settlement.

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

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

17. Monitoring of Transactions

a Regular monitoring of transactions is vital for ensuring effectiveness of the KYC/AML/CFT procedures. The Company shall have an understanding of the normal activity of the Client so that it can identify deviations in transactions/ activities.

b 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 in its SOP 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 PFRDA/ FIU-India/ 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.

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

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

18. Consequence Management in case of non-compliance

- In terms of Section 13 of the Act, the Director, FIU-India can take appropriate action, including imposing a monetary penalty on company or Designated Director or any of its employees for failure to comply with any of its AML/CFT obligations

- As per the Company's core principle on AML, Company staff who act in breach with the Policy and who may expose the Company to AML related risks shall be dealt with seriously in accordance with the employee disciplinary action process and the law.

- When faced with a non-compliant intermediary, the Company shall take necessary action to secure compliance. Services of defaulting intermediaries who expose the Company to AML/CFT related risks on multiple occasions, appropriate action should be initiated.

19. Policy Ownership

The Principal Officer is responsible for overseeing the implementation of compliance to this Policy. Please contact your department head for any clarifications or write to compliance team for further queries on this Policy.

Annexure I: Definitions and Abbreviations

a. "**Act**" means the Prevention of Money Laundering Act, 2002, as amended from time to time.
b. "**Company**:" means Max Life Pension Fund Management Company Limited.
c. "**Client**" means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who engaged in the transaction or activity, is acting.
   Note - The phrase subscriber, customer and Client has been used interchangeably and shall be considered to have the same meaning.
d. "**Equivalent e-document**" 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;
e. **"Money Laundering"** Section 3 of the Act defines the "offence of money laundering" as under:

   Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering."

   As per the Guidelines, money laundering is a process or activity through which proceeds of crime (i.e., illegally acquired money) are converted in the financial systems (by means of undertaking transactions) so that it appears to be legally acquired

   There are three common stages of money laundering as detailed below which are resorted to by the launderers and insurance institutions may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions:

   - *Placement* – the disposal of cash proceeds derived from an illegal activity;
   - *Layering* – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and
   - *Integration* – creating the impression of apparent legitimacy to criminally derived wealth

   If the layering process has succeeded, integration schemes place the laundered proceeds back into economy in such a way that they re-enter the financial system appearing to be normal business funds. Financial institutions such as insurers are therefore, placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through such institution.
f. "**Politically Exposed Persons**"/ (**PEPs**) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., heads of states/ governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc..

g. "**Principal Officer" or "PO**": means any officer at a senior level appointed by the Company to ensure compliance with the obligations imposed under Chapter IV of the Act and the Rules.
h. "**Rules**" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time.
i. "**Transaction**": includes deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.
j. "**Video Based Customer Identification Process** (**VCIP**)" means an alternative (optional) electronic process of Identification/ KYC in paperless form, carried out by the Company by undertaking seamless, secure, real-time with geotagging, consent based audio-visual interaction with the subscriber to obtain identification information including the necessary KYC documents required for the purpose of CDD and to ascertain the veracity of the information furnished by the Client.

A list of key abbreviations used in this Policy is set out below:

AML	Anti-Money Laundering
APY	Atal Pension Yojana
CFT	Counter-Financing of Terrorism
KYC	Know Your Customer
FIU-India	Financial Intelligence Unit of India
FATF	Financial Action Task Force
STR	Suspicious Transaction Report
CTR	Cash Transaction Report
CCR	Counterfeit Currency Report
PAN	Permanent Account Number
PFRDA	Pension Fund Regulatory and development Authority
UIDAI	Unique Identification Authority of India
NREGA	National Rural Employment Guarantee Act
NPS	National Pension Systems
OVD	Official Valid Document
PRAN	Permanent Retirement Account Number
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India