Date: 23rd November, 2022

To

All Stakeholders,

Subject: Draft guidelines in respect of Know Your Customer /Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT), 2022.

Authority is in process of drafting guidelines in respect of Know Your Customer /Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT), 2022. These guidelines cover the provisions of PML Act, PML Rules and are applicable to Point of Presence.

2. You are requested to submit your feedback / inputs till **08th December, 2022** in the below format to following email ids:
devesh.mittal@pfrda.org.in
ashish.bharati@pfrda.org.in

Format for Suggestion on Exposure Draft in respect of *Know Your Customer / Anti – Money Laundering / Combating the Financing of Terrorism (KYC / AML / CFT), 2022*

Designation and Organisation:				
Name and contact number:				
Sr.	Wordings of the Regulation as per Exposure Draft	Page No. and Para No.	Proposed Change(s)	Rationale for proposed change / Comment

Guidelines in respect of Know Your Customer / Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT), 2022

1. Short Title

These guidelines shall be called as Guidelines in respect of Know Your Customer **/** Anti-Money Laundering / Combating the Financing of Terrorism (KYC/AML/CFT), 2022. These guidelines are issued by exercising the power conferred under Section 14(1) of Pension Fund Regulatory and Development Authority Act, 2013(PFRDA Act) and provisions 4,5,7,9, 9A & 10 of the PML Rules.

2. Introduction

2.1 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. Section 3 of PML Act specifies the Offence of Money Laundering.

2.2 In terms of the provisions of Prevention of Money Laundering Act, 2002 (PML Act) and the Prevention of Money Laundering (Maintenance of records) Rules, 2005 (PML Rules), reporting entities (RE) are 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-going basis.

2.3 The obligation to establish an anti-money laundering mechanism and formulate and implement a Client Due Diligence (CDD) Programme applies to RE as per provisions of clause (ii) and (iii) sub rule (14) of Rule 9 of the PML Rules. RE 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.

2.4 All REs shall take steps to implement provisions of the PML Act and the PML Rules, as amended from time to time, including operational instructions issued through circulars/guidelines/ directions in pursuance of such amendment(s).

3. Definitions

In these guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

3.1 **"**Aadhaar number", shall have the meaning assigned to it under clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter referred to as "Aadhaar Act".

3.2 "Act / PML Act / PMLA" means the Prevention of Money Laundering Act, 2002.

3.3 “Authentication”, means the process as defined under clause (c) of section 2 of the Aadhaar Act.

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

3.5 “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.

3.6 “Client” shall have the meaning assigned to it under clause (ha) of sub section (1) of Section 2 of the PML Act.

3.7 “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.

3.8 “Designated Director" shall have the meaning assigned to it under clause (ba) of sub-rule (1) of Rule 2 of the PML Rules.

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

3.10 “Equivalent e-document” shall have the meaning assigned to it under clause (cb) of sub-rule (1) of Rule 2 of the PML Rules.

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

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

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

3.14 “Non-face-to-face customers” shall have the same meaning assigned to it under sub clause (ix) of 3(b) of Chapter I of Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.

3.15 “Offline verification” shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act.

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

3.17 "Officially valid document" shall have the meaning assigned to it under clause (d) of sub-rule (1) of Rule 2 of the PML Rules.

3.18 “Politically Exposed Persons” (PEPs) shall have the same meaning assigned to it under sub clause (xii) of 3(b) of Chapter I of Master Direction – Know Your

Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.

3.19 "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.

3.20 "Principal Officer" shall have the same meaning assigned to it under clause (f) of sub-rule (1) of Rule 2 of the PML Rules.

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

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

3.23 "Suspicious Transaction" shall have the meaning assigned to it under clause (g) of sub-rule (1) of Rule 2 of the PML Rules.

3.24 "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.

3.25 "Customer / Subscriber" shall have the meaning as per clause (t) of sub-section (1) of section 2 of the PFRDA Act.

3.26 Words and expressions used and not defined in these guidelines 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.

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

4.1 Every reporting entity, has to establish and implement policies, procedures, internal controls and formulate and implement a Client Due Diligence (CDD) Programme that effectively serve to prevent and impede Money Laundering (ML) and Terrorist Financing (TF).

4.2 To be in compliance with these obligations, the senior management of every reporting entity shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The reporting entities shall:

4.2.1 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.

4.2.2 Ensure that the content of these guidelines are 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.

4.2.3 The KYC/AML/CFT program should have the approval of the Board of Directors or equivalent authority of RE. The program should 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.

4.2.4 The Board of Directors or equivalent authority or Committee of the Board or the Senior Management Official(s) designated by the Board shall be apprised about the observations, violations, reporting etc., including follow-up action about the decision to continue or exit the relationship on periodic basis.

4.2.5 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.

4.2.6 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

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

4.3.1 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 reporting entities;

4.3.2 The Client Due Diligence Program including policies, controls and procedures, approved by the Board of Directors or equivalent authority or Committee of the Board or the Senior Management Official(s) designated by the Board to enable the reporting entities to manage and mitigate the risk that have been identified by the reporting entities;

4.3.3 Maintenance of records;

4.3.4 Compliance with relevant statutory and regulatory requirements;

4.3.5 Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;

4.3.6 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.

4.4 Responsibility of reporting entities:

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

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

4.4.2 Reporting entities shall initiate appropriate actions against defaulting representative of reporting entity who expose the reporting entities to KYC/AML/CFT related risks on multiple occasions.

4.4.3 As some reporting entities are 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.

4.5 Certificate of Compliance:

Reporting entities shall submit certificate of compliance as provided in **Annexure I** within 45 days from end of each Financial Year.

5. Appointment of a Designated Director and a Principal Officer

5.1 A “Designated Director”, who has to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules, shall be appointed or designated by the reporting entities.

5.2 A “Principal Officer” (PO) at a senior management shall be appointed to ensure compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules.

5.3 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 from the date of issuance of these guidelines to Pension Fund Regulatory and Development Authority (PFRDA) and FIU-IND. Any changes thereon shall be communicated to PFRDA and FIU-IND within 7 days of its effect.

Provided further that any entity (falling under the definition of RE) shall at the time of making application for fresh registration, submit the details as mentioned above.

5.4 In terms of Section 13 of the PML Act, the Director, FIU-IND can take appropriate action, including imposing a monetary penalty on reporting entities or its Designated Director or any of its employees for failure to comply with any of its KYC/AML/CFT obligations.

6. Recruitment and Training

6.1 Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

6.2 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 reporting entities, guideline and related issues shall be ensured.

7. Internal Control/Audit

Internal audit/inspection department of reporting entities or the external auditor appointed by RE shall periodically verify compliance with the extant policies, procedures and controls related to money laundering activities on the basis of overall risk assessment. Reporting entities shall 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. Reporting entities shall submit audit notes and compliance to the Audit Committee and in its absence directly to the Board or equivalent authority of the RE.

8. Know Your Customer (KYC) Norms

8.1 KYC Norms

8.1.1 Reporting entities should make best efforts to determine the true identity of subscriber(s).

8.1.2 No reporting entity shall 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).

8.1.3 Reporting entities shall verify the identity, address and recent photograph in compliance with provision as specified in PML Rules.

8.1.4 At any point of time, where reporting entities are 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.

8.1.5 Reporting entities may perform KYC process by any of the following methods:

8.1.5.1 Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PML Act Or

8.1.5.2 Aadhaar based KYC through offline verification Or

8.1.5.3 Digital KYC as per PML Rules Or

8.1.5.4 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 (Annexure 2) Or

8.1.5.5 By using "KYC identifier" allotted to the subscriber by the CKYCR Or

8.1.5.6 By "using Digilocker" as prescribed by the PFRDA vide circular no. PFRDA/2021/5/PDES/5 dated 3rd Feburary 2021 (Annexure 3) Or

8.1.5.7 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

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

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

8.2 Client Due Diligence (CDD)

Reporting entity shall undertake CDD as per the provisions of Rule 9 of PML Rules. Accordingly, the reporting entities shall undertake CDD as follows:

8.2.1 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.

8.2.2 Knowing existing subscribers

8.2.2.1 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 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) / relative of PEP / close associate of PEP / nominee 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 subscriber.
e. As and when there are revision or changes in PML Act / PML Rules.

8.2.2.2 Where the risks of money laundering or terrorist financing are higher, reporting entities should be required to conduct enhanced due diligence (EDD) measures, consistent with the risks identified.

8.2.3 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.

8.2.3.1 Reporting entity shall identify the source of contribution and ensure that the contribution is being done through the subscriber's own source of funds.

8.2.3.2 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.

8.2.3.3 Notwithstanding the above, reporting entities are 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.

9. Risk Assessment and Risk Categorization

9.1 Pension Accounts are generally considered as low risk accounts. However, the risk assessment of subscribers under pensions schemes regulated / administered by PFRDA may *inter-alia* take into account the following :

9.1.1 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)

9.1.2 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)

9.1.3 Contributions towards NPS Tier I account on a voluntary basis (These accounts generally involve moderate risk)

9.1.4 Voluntary contributions towards NPS Tier II account, which is a withdrawable account (These accounts involve generally higher risk in comparison to other categories)

9.2 Notwithstanding anything contained in 9.1 above, while assessing the subscriber's risk profile RE shall consider the following factors:

9.2.1 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)

9.2.2 Source of contribution

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

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

9.2.5 Withdrawals under Tier I and Tier II account

9.2.6 Residence status of subscriber (For eg – Subscribers residing in jurisdiction with higher national risk assessment)

9.2.7 Political Exposed Person

9.2.8 Contributions made by the subscriber vis-à-vis the declared income/ income range

Above list is indicative and not exhaustive. RE may consider additional factors using its own judgement and past experience.

9.3 Reporting entities 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 reporting entities are 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 reporting entities should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

9.4 The documented risk assessment shall be updated from time to time. The reporting entities 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.

9.5 Risk Categorization:

9.5.1 Risk categorization shall be undertaken based on parameters detailed at clause 9.1 and 9.2 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. RE shall ensure enhanced due diligence (EDD) for NPS Tier II account (except accounts under NPS Tier II Tax Saver Scheme)

9.5.2 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 PRAN account may require only the basic requirements like verifying the identity, current address, annual income and sources of 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 subscribers profile is inconsistent with the investment through subsequent contributions, a re-look on subscribers profile is to be carried out.

9.5.3 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.

10. Simplified Due Diligence (SDD)

10.1 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 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.

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

11. Enhanced Due Diligence (EDD)

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

11.2 Reporting entities 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, reporting entities should be required to conduct enhanced due diligence measures, consistent with the risks identified.

11.3 Reporting entities shall

11.3.1 Verify the identity of the subscriber preferably using Aadhaar subject to the consent of subscriber or;

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

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

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

12.1 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.

12.2 The Reporting entities are required to perform the CKYCR related functions in the manner as prescribed under the PML Rules. For the purpose of performing such functions the REs are required to get registerd with CERSAI. Presently, under the NPS architecture the Reporting entities 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, REs already registered with CERSAI under another financial sector regulator are not required to register themselves with CERSAI again, and may use such registration with CERSAI as reporting entities under PFRDA as well.

12.3 Where a subscriber submits a "KYC identifier" for KYC, the reporting entities 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 reporting entities as per Rule 9(1C) of PML Rules.

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

12.5 If the KYC identifier is not submitted by the subscriber or not available in the CKYCR portal, reporting entities shall capture the KYC information in the manner as prescribed under the 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

12.6 Reporting entities 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.

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

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

12.8.1 For online Authentication,

a) The redacted Aadhar Number (Last four digits)

b) Demographic details

c) The fact that Authentication was done

12.8.2 For offline Verification

a) KYC data

b) Redacted Aadhaar number (Last four digits)

12.9 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. Reporting entities shall upload the updated KYC data pertaining to active pension accounts against which "KYC identifier" are yet to be allotted/generated by the CKYCR.

12.10 Reporting entities 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).Reporting entity 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)

12.11 Reporting entity shall submit the MIS related to the CKYC data upload/ download etc. to PFRDA as stipulated from time to time.

13 Reliance on third party KYC

13.1 For the purposes of KYC norms under clause 8, while reporting entities are ultimately responsible for subscriber due diligence and undertaking enhanced due diligence measures, as applicable, reporting entities 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. Where reporting entity relies upon third party that is part of the same financial group, they should obtain KYC documents or the information of the subscriber due diligence within 15 days.

13.2 Reporting entities can utlise the SEBI KRA for KYC in accordance with PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019 (Annexure 4)

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

14 Pension accounts of Politically Exposed Persons (PEPs)

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

14.2 Reporting entities are 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. These measures are also to be applied to pension accounts of which a PEP is the ultimate beneficiary / nominee.

14.3 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.

14.4 Reporting entities 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 reporting entity that processes exit request should apply risk-based monitoring of such withdrawal to determine if the recipient of the funds is a PEP.

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

15.1 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.

15.2 The reporting entities 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.

15.3 Reporting entities shall periodically check MHA website for updated list of banned individuals.

15.4 Reporting entities 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.

15.5 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.

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

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

Reporting entities are required to:

16.1 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.

16.2 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.

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

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

16.5 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).

17 Reporting Obligations

17.1 RE 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.

17.2 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 reporting entities which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those reporting entities, 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.

17.3 Red Flag Indicators issued by FIU-IND also be taken in account for Suspicious Transaction, wherever necessary.

17.4 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. Reporting entities shall not put any restriction on operations in the accounts where an STR has been filed. Reporting entities 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.

17.5 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.

17.6 Reporting entities 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.

17.7 Reporting entities 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.

18 Record Keeping

18.1 In view of Rule 5 of the PML rules, the reporting entities, 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) reporting entities are 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.

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

18.2.1 Reporting entities 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.

18.2.2 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.

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

18.2.4 It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.

18.3 Reporting entities 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. Reporting entities should retain the records of those accounts, which have been settled by claim, for a period of at least five years after that settlement.

18.4 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, reporting entities are required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.

18.5 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.

19 Monitoring of Transactions

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

19.2 Reporting entities shall pay special attention to all complex large transactions/ patterns which appear to have no economic purpose . The reporting entities 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.

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

19.4 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.

20 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.

21 The reporting entities are 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.

Annexure I

(As specified in 4.5)

Certificate of Compliance (Guidelines on KYC/AML/CFT)

Name of Reporting Entity:

Financial Year:

We do hereby submit that our company ..... (name of the reporting entity) has fully complied with all the norms laid down under KYC/AML / CFT guidelines 2022, and the company has set up a robust mechanism to comply with the extant PML Act / PML Rules.

Designated Director (Name and Signature)

(* to be submitted within 45 days of end of FY)

Appendix

List of Circulars or part thereof repealed with the issuance of Guidelines

Sl no	Circular no	Subject	Date
1	PFRDA/2019/14/PDES/1	Point of Presence (PoP) relying on third party client due diligence (KYC) for onboarding subscribers in NPS	24th July 2019
2.	PFRDA/2021/11/SUP-POP/1	Central KYC Records Registry (CKYCR)	22nd April 2021
3.	PFRDA/2021/31/SUP-POP/4	Central KYC Records Registry (CKYCR)	26th July 2021