FAQs on KYC/AML/CFT guidelines issued by PFRDA

1. What is the purpose of these guidelines in the context of the National Pension System (NPS)?

These guidelines are designed to ensure compliance with Know Your Customer (KYC), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) measures within the NPS. They outline procedures for identifying customers, monitoring transactions, and preventing unlawful financial activities. **(Para 1)**

2. What is money laundering, and how does it relate to the NPS?

Money laundering is the process by which illegally acquired funds are made to appear legally acquired within the financial system. The guidelines acknowledge that the Prevention of Money Laundering Act, 2002 (PML Act), and related rules apply to reporting entities (RE) within the NPS to prevent money laundering and terrorist financing activities. **(Para 2.2)**

3. What are Customer Identification Procedures (CIP), and when are they applied within the NPS?

Reporting entities (RE) within the NPS are required to follow Customer Identification Procedures (CIP) when establishing an account-based relationship or client-based relationship. These procedures are aimed at verifying the identity of customers and monitoring their transactions on an ongoing basis. **(Para 2.3)**

4. What is the responsibility of reporting entities (RE) regarding anti-money laundering and client due diligence?

Reporting entities (RE) within the NPS have a responsibility to establish an anti-money laundering mechanism and implement a Client Due Diligence (CDD) Programme in accordance with the provisions of the Prevention of Money Laundering (Maintenance of records) Rules. REs must guard against the misuse of NPS and ensure it is not used for unlawful fund laundering or financing of terrorist acts. **(Para 2.4)**

5. What is a Client Due Diligence (CDD) Programme, and why is it important?

A CDD Programme is a set of policies and procedures designed to identify, assess, and manage the risk of ML and TF. It is crucial for reporting entities to have an effective CDD Programme in place to prevent and impede ML and TF activities. **(Para 4.1)**

6. What components should be included in a KYC/AML/CFT program?

A KYC/AML/CFT program should include policies and procedures related to KYC (Know Your Customer), ML, and TF. It should reflect current statutory and regulatory requirements and be approved by the Board of Directors or equivalent authority. **(Para 4.2.1 & 4.2.3)**

7. How should reporting entities handle suspected ML or TF transactions?

Reporting entities should have a system in place to identify, monitor, and report suspected ML or TF transactions to the Financial Intelligence Unit – India (FIU-IND) and law enforcement authorities in accordance with government guidelines. **(Para 4.2.6)**

8. What responsibilities do reporting entities have in ensuring compliance with these guidelines?

Reporting entities are responsible for establishing Standard Operating Procedures, monitoring and taking action against defaulting representatives, and scrutinizing the engagement process of individuals like business correspondents or agents who are facilitating the distribution of pension schemes.
Reporting entities are required to submit a Certificate of Compliance along with their Annual Compliance Certificate to demonstrate adherence to these guidelines. **(Para 4.4 to 4.4.3 & 4.5)**

9. Who is a "Designated Director," and "Principal Officer" and what is their role?

"Designated Director" is responsible for ensuring overall compliance with the obligations under Chapter IV of the PML Act and the PML Rules within reporting entities.

The Principal Officer is a senior management position responsible for ensuring compliance with the obligations under Chapter IV of the PML Act and the PML Rules. **(Para 5.1 & 5.2)**

10. How should reporting entities inform PFRDA and FIU-IND about the contact details of the Designated Director and Principal Officer?

Reporting entities must submit the contact details of these individuals within 30 days of the issuance of these guidelines, and any changes must be communicated within 30 days of taking effect. **(Para 5.3)**

11. What actions can be taken by the Director, FIU-IND, for non-compliance with KYC/AML/CFT obligations?

The Director, FIU-IND, has the authority to take appropriate actions, including imposing monetary penalties on reporting entities, Designated Directors, or employees for failing to comply with their KYC/AML/CFT obligations. **(Para 5.4)**

12. How can reporting entities ensure that their personnel are adequately trained in KYC/AML/CFT policies?

Reporting entities should establish ongoing training programs tailored to different staff categories (frontline, compliance, etc.) to ensure they are well-versed in KYC/AML/CFT policies. **(Para 6.1 & 6.2)**

13. What is the role of internal audit/inspection departments or external auditors in compliance?

Internal audit/inspection departments or external auditors must periodically verify compliance with policies and controls related to money laundering activities and submit reports to the Audit Committee or the Board of Directors. These reports should assess the robustness of internal policies and processes and provide constructive suggestions for improvement. **(Para 7)**

14. What is the purpose of KYC norms for reporting entities?

KYC norms are established to ensure that reporting entities make their best efforts to determine the true identity of subscribers, thereby preventing money laundering (ML) and terrorist financing (TF) activities. Reporting entities are prohibited from allowing the opening of or maintaining anonymous or fictitious accounts. **(Para 8.1.1 & 8.1.2)**

15. What is a Suspicious Transaction Report (STR)?

An STR is a report filed by a reporting entity to the Financial Intelligence Unit (FIU) when it forms a suspicion of money laundering or terrorist financing. It is a critical tool for reporting suspicious activities to the authorities.

16. When should reporting entities file a Suspicious Transaction Report (STR)?

Reporting entities should file an STR with the Financial Intelligence Unit-India (FIU-IND) when they are no longer satisfied about the true identity and transactions of a subscriber, provided the transaction meets specific criteria outlined in the rules and guidelines issued by FIU-IND or PFRDA. **(Para 8.1.4)**

17. What methods can reporting entities use for performing KYC processes?

Reporting entities can perform KYC processes using various methods, including Aadhaar-based KYC, digital KYC, Video-Based Customer Identification Process (VCIP), KYC identifier, Digilocker, certified copies of valid documents, PAN/Form 60, and other required documents. **(Para 8.1.5.1 to 8.1.5.8)**

18. How often should KYC be updated for existing subscribers?

For existing subscribers 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. **(Para 8.2.2.1)**

19. When should a reporting entity opt to file a Suspicious Transaction Report (STR) instead of pursuing the Client Due Diligence (CDD) process?

If a reporting entity forms a suspicion of money laundering or terrorist financing and reasonably believes that continuing the Client Due Diligence (CDD) process might alert the customer, they should refrain from CDD and promptly file an STR with Financial Intelligence Unit. **(Para 8.2.2.3)**

20. How should reporting entities handle payments upon superannuation or pre-mature exit or death?

Payments upon superannuation or premature exit or death should not be made to third parties, except to nominee(s) or legal heir(s) in the case of death. Due diligence of the recipient(s) should be carried out before making payments or settling claims. **(Para 8.2.3.2)**

21. What factors are considered for risk assessment and categorization of subscribers?

Factors considered for risk assessment include the nature of the account, source and mode of contribution, regularity in contributions, withdrawals, residence status, Politically Exposed Person (PEP) status, declared income, and more. Based on above, subscribers are categorized as low-risk, moderate-risk, or high-risk, depending on their profile and activity. **(Para 9.1 & 9.2)**

22. What are the KYC requirements for low-risk subscribers?

Low-risk subscribers may have basic KYC requirements, including verifying identity, current address, annual income, and the source of funds. Periodic reviews may be conducted if the subscriber's profile is inconsistent with their contributions. **(Para 9.5.2)**

23. What KYC procedures should be in place for high-risk subscribers?

High-risk subscribers, such as non-residents, high net worth individuals, and politically exposed persons (PEPs), require higher verification and counter checks to ensure compliance with KYC procedures. **(Para 9.5.3)**

24. When can reporting entities apply Simplified Due Diligence (SDD)?

SDD can be applied to APY accounts classified as Low Risk. However, it should not be used when there is suspicion of money laundering or terrorist financing or in specific high-risk scenarios as determined by the Risk Assessment/categorization policy of the reporting entities. **(Para 10.1)**

25. What documents are required for SDD as per PML Rules?

The list of documents required for SDD is specified in clause (d) of sub-rule (1) of Rule 2 of the PML Rules. These documents are designed to simplify the KYC process for low-risk accounts. **(Para 10.2)**

26. When should reporting entities conduct Enhanced Due Diligence (EDD)?

Reporting entities should conduct EDD for high-risk subscribers and in cases where there are unusual patterns of transactions with no apparent economic or lawful purpose. **(Para 11.1 & 11.2)**

27. How can reporting entities verify the identity of subscribers during EDD?

Reporting entities can verify the identity of subscribers during EDD preferably using Aadhaar, subject to the subscriber's consent. Alternatively, they can use other methods of KYC as specified through circulars or guidelines issued by the Authority. **(Para 11.3)**

28. Which reporting entities are required to register with Central KYC Registry (CKYCR)?

Under NPS architecture the Reporting entities registered under regulation 3(1)(i) and regulation 3(1)(ii) of PFRDA (Point of Presence) Regulations, 2018 should register with CKYCR. Entities already registered with CKYCR under another financial sector regulator are not required to register again. **(Para 12.2)**

29. How can reporting entities retrieve KYC records from CKYCR using a "KYC identifier"?

Reporting entities can retrieve KYC records from CKYCR when a subscriber submits a "KYC identifier." This eliminates the need for the subscriber to submit KYC records again unless there is a change in the required information. **(Para 12.3)**

30. What information should reporting entities upload to CKYCR during the account-based relationship commencement?

Reporting entities should upload an electronic copy of the subscriber's KYC records to CKYCR within 10 days of commencing the account-based relationship. They should follow guidelines and instructions provided by PFRDA for this purpose. **(Para 12.6)**

31. What details need to be uploaded on CKYCR for Aadhaar verification/authentication?

For online authentication, reporting entities should upload the redacted Aadhaar number (last four digits), demographic details, and the fact that authentication was done. For offline verification, KYC data and the redacted Aadhaar number (last four digits) should be uploaded. **(Para 12.8.1 & 12.8.2)**

32. Can reporting entities use KYC records obtained from CKYCR for purposes other than identity or address verification?

Reporting entities should not use KYC records obtained from CKYCR for any purposes other than verifying the identity or address of the subscriber, unless authorized by the subscriber, PFRDA, or the Director (FIU-IND). **(Para 12.10)**

33. Can reporting entities rely on third-party KYC for subscriber due diligence?

Reporting entities can 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. However, they are ultimately responsible for subscriber due diligence.
Reporting entities can utilize the SEBI KRA (KYC Registration Agency) for KYC reliance, as outlined in the PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019. **(Para 13.1 to 13.3)**

34. What should reporting entities do if they identify a subscriber or beneficiary as a PEP during ongoing risk management?

Reporting entities should inform senior management of the business relationship involving a PEP and apply enhanced due diligence measures.
Reporting entities must take reasonable steps to determine the origin of wealth and funds for subscribers identified as PEPs. **(Para 14.3 & 14.5)**

35. What is the purpose of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)?

Section 51A of the UAPA relates to the prevention of and coping with terrorist activities. It was introduced through the UAPA Amendment Act, 2008. The purpose of Section 51A is to empower the Central Government to freeze, seize, or attach funds and prevent entry into or transit through India of individuals or entities suspected to be engaged in terrorism. **(Para 15.1 & 15.5)**

36. Are reporting entities allowed to open pension accounts for individuals on the UN sanction list or those with terrorist links?

No, reporting entities should not open pension accounts for individuals whose identity matches with any person on the UN sanction list or those reported to have links with terrorists or terrorist organizations.
Reporting entities should periodically check the Ministry of Home Affairs (MHA) website for updated lists of banned individuals and designated individuals. **(Para 15.2 & 15.3)**

37. How can reporting entities access the United Nations' lists of individuals and entities subject to sanctions?

Reporting entities can access the lists of individuals and entities subject to various sanction measures established pursuant to UNSC 1267 and UNSC 1988 from the United Nations' website at the provided URLs. **(Para 15.4)**

https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

https://www.un.org/securitycouncil/sanctions/1988/materials

38. What is the requirement for reporting entities regarding individuals residing in countries with AML/CFT deficiencies?

Reporting entities must conduct enhanced due diligence before establishing an account-based relationship with individuals residing in countries identified by FATF as having deficiencies in their AML/CFT regime. They should thoroughly examine the unusual contributions, the background and purpose of such transactions and maintain written findings. **(Para 16.1 & 16.2)**

39. Who is responsible for filing reports to the Director, FIU-IND in accordance with PML Rules for NPS?

The Central Recordkeeping Agency (CRA) is responsible for filing reports to the Director, FIU-IND in accordance with PML Rules for NPS.
Reporting entities must furnish information referred to in Rule 3 of the PML Rules in terms of Rule 7 thereof. The Director, FIU-IND has the authority to issue guidelines for detecting transactions and specify the procedure and manner of furnishing information. **(Para 17.1 & 17.2)**

40. Where can reporting entities find reporting formats and guidelines for filing reports to FIU-IND?

Reporting formats, a comprehensive reporting format guide, and electronic utilities for filing electronic Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) can be found on the FIU-IND website. **(Para 17.3)**

41. How should reporting entities handle suspicious transactions?

Reporting entities should ensure that suspicious transactions are promptly reported to the Director, FIU-IND. They should also maintain confidentiality and not tip off the subscriber regarding the filing of STRs. **(Para 17.5)**

42. How long should reporting entities maintain transaction-related records?

Reporting entities, including their designated directors, principal officers, and employees, must maintain records (electronic/physical form) of all transactions and subscriber identity verification for a period of five years. **(Para 18.1 & 18.2)**

43. What criteria should reporting entities consider when utilizing third-party service providers for record maintenance?

Reporting entities should ensure that third-party service providers have the organizational capabilities, technology, and security measures in place to safeguard data privacy and prevent unauthorized access and disclosure. **(Para 18.2)**

44. What should reporting entities pay special attention to in transactions?

Reporting entities should pay special attention to complex large transactions or patterns without apparent economic purpose. They should also establish internal threshold limits for subscriber accounts and examine transactions exceeding these limits. **(Para 19.2)**