Annexure - B
(Part-I Policy)

Policy for Know Your Customer (KYC)

Division : Data Privacy & Management Division
Version : 2025_KYC_1.1

Policy Custodian

Division	Data Privacy & Management Division
Officer in-charge	General Manager
Policy Contact	kyc@pnb.co.in

Policy Version Control

S.N.	Version Number	Version Date	Summary of Changes
1	2022_KYC_1.0	29 March 2022	Periodic updation, Customer Due Diligence
2	2023_KYC_1.0	29 March 2023	ML and TF risk assessment, Reports to be furnished to Financial Intelligence Unit – India, Internal control system.
3	2023_KYC_1.1	11 May 2023	Policy updated as per RBI, Master Directions dated 28.04.2023 & 04.05.2023, GOI (MOF) Gazette Notification dated 03.05.2023 &09.05.2023
4	2023_KYC_1.2	01 Nov 2023	Policy updated as per RBI, Master Directions dated 17.10.2023
5	2024_KYC_1.0	27 Feb 2024	Enhanced Due Diligence – Accounts of Politically exposed persons, Periodic Updation
6	2024_KYC_1.1	10 December 2024	PFRDA Master Direction on KYC for NPS as per PFRDA/Master Circular/2024/04/PoP-02 dated 23.01.2023 updated as on 10.04.2024.
7	2025_KYC_1.0	19 March 2025	RBI updated its Master Direction –Know Your Customer (KYC) Direction, 2016 on updated 06.11.2024 and PFRDA updated its Master Direction on 23.09.2024.
8	2025_KYC_1.1		RBI updated its Master Direction – Know Your Customer Direction, 2016 on 12.06.2025.

Policy Governance

Frequency Of Review	Annual
Last reviewed on	19.03.2025
Approval Path	ACE >ACB> Board
Supersedes	Data Privacy & Management Division Circular No. 13/2025 dated 19.03.2025

Contents

1. POLICY OVERVIEW

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India and other Laws/ Regulations, Bank is required to follow certain customer identification procedure while undertaking a transaction, either by establishing an account-based relationship or otherwise and monitor their transactions. This KYC Policy is issued as per RBI's Master Direction on Know Your Customer updated up to 12.06.2025 and as per PFRDA Master Direction on KYC /AML/CFT updated up as on 23.09.2024.

2. POLICY DETAILS

2.1 BACKGROUND

Know Your Customer Policy of the Bank framed in accordance with RBI's Master Direction on KYC, updated as on 06.11.2024 and as per PFRDA Master Direction on KYC /AML/CFT updated up as on 23.09.2024, was last approved by the Board in its meeting held on 28.02.2025. Accordingly, KYC Policy of the Bank was circulated vide Data Privacy and Management Division Circular No. 13/2025 dated 19.03.2025.

In compliance to the provisions of the RBI guidelines on KYC, the present policy is being framed and placed as Part-I Policy Guidelines and Part-II Operational Guidelines of KYC Policy.

2.2 OBJECTIVES AND PURPOSE

India, being a member of Financial Action Task Force (FATF) is committed to upholding measures to protect the integrity of international financial system. To prevent Bank from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of various rules and regulations. The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:

i. To prevent Bank from being used intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the vcip know/understand their customers and their financial dealings better, which in turn helps it to manage the

associated risks prudently.

ii. To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank's Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

iii. The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

iv. For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

2.3 SCOPE AND APPLICABILITY

2.3.1 Scope and applicability of KYC Policy of the Bank-

i) All offices of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s). The provisions of KYC Policy guidelines shall apply to all the branches / offices of the Bank/Point of Presence-Service Providers (PoP-SP), NPS Trust and Retirement Advisers.

ii) The guidelines in this circular apply to the branches and majority owned subsidiaries located abroad, to the extent they are not contradictory to the local laws in the host country, provided that:

a) Where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India.

b) In case there is a variance in KYC / AML standards prescribed by the Reserve Bank of India and the host country regulators, branches / overseas subsidiaries of Bank are required to adopt the more stringent regulation of the two.

Above guidelines however shall not apply to 'small accounts' referred to in Section 5 of Part-II, Operational Guidelines for KYC.

2.3.2 Point of Presence (PoP) for National Pension System

Our Bank is registered as a Point of Presence (PoP) with PFRDA and our branches act as Point of Presence-Service Provider (POP-SP) for assisting the individuals for the purpose of subscriber registration, fund collection, and servicing of other requests related to National Pension System (NPS).
Entities registered as Point of Presence (PoP) are required to comply with the requirements of Prevention of Money Laundering Act, 2002 as per Regulation 15 of the PFRDA (Point of Presence) Regulations, 2018.

National Pension System (NPS) has an unbundled Architecture, where each function is performed by different intermediaries appointed by the PFRDA viz. Pension Funds, Custodian, Central Recordkeeping Agency (CRA), National Pension System Trust, Trustee Bank, Points of Presence (PoP), Retirement Advisers (RAs) and Annuity Service Providers (ASPs) registered with Insurance Regulatory and Development Authority of India (IRDAI). Wherein, the role of CRA is recordkeeping, administration and customer service functions for all the subscribers of the NPS including issuance of unique Permanent Retirement Account Number (PRAN) to each subscriber, maintaining a database of all PRANs issued and recording transactions relating to each subscriber's PRAN.

2.3.3 **Implementation of group-wide policy**- In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002 (15 of 2003). Accordingly, every RE which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off. CAML Cell, FRMD Division shall formulate Policy and SOP to implement the same.

2.3.4 Bank's policy framework shall seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, it shall also be considered to adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

2.4 POLICY CONTENTS

2.4.1 THE KYC POLICY INCLUDES FOLLOWING KEY ELEMENTS:

a) CUSTOMER ACCEPTANCE POLICY

2.4.1.1 Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of customers. It is to be ensured as under: -

(i) No account is opened in anonymous or fictitious / benami name.
(ii) No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. STR shall be filed if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer**.**
(iii) No transaction or account-based relationship is undertaken without following the CDD procedure.
(iv) The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
(v) Additional information, where such information requirement has not been specified in KYC Policy of the Bank, is obtained with the explicit consent of the customer.
(vi) The CDD procedure is to be applied at the UCIC level. Thus, if an existing KYC compliant customer of a Bank desires to open another account or avail any other product or service from the same Bank, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
(vii) CDD Procedure is followed for all the joint account holders, while opening a joint account.
(viii) Circumstances, in which a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
(ix) No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the Master Direction of RBI on KYC as amended from time to time.
(x) Where Permanent Account Number (PAN) is obtained, the same shall beverified from the verification facility of the issuing authority.
(xi) Where an equivalent e-document is obtained from the customer, the digital signature has to be verified as per the provisions of the Information Technology Act, 2000 (21 of 2000).
(xii) Where Goods & Services Tax (GST) details are available, the GST

number shall be verified from the search/ verification facility of the issuing authority.

2.4.1.2 It is to be ensured that the Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

2.4.1.3. Where a suspicion of money laundering or terrorist financing, is formed and reasonably believed that performing the CDD process will tip-off the customer, CDD process shall not be pursued, instead it shall be reported to Centralised AML Cell for onward submission of STR to FIU –IND.

b) RISK MANAGEMENT

For Risk Management, Bank has adopted risk-based approach which includes the following:

(i) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Bank.

(ii) Broad principles may be laid down by the Bank for risk-categorization of customers.

(iii) Risk categorization shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and information about the clients' business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken—cash, cheque/ monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

(iv) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

It is hereby specified that the various other information collected from different categories of customers, relating to the perceived risk, is non-intrusive. Lists such as FATF Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association (IBA), and other agencies, etc., have been used in risk assessment.

Risk Categorization under NPS

A. New Subscriber (Customer):

NPS customers will be classified in the following risk categories:

i. **Low Risk -** 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 (customers), 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. Employees of central / state government / autonomous bodies / public sector undertakings covered under NPS are classified under low risk category.

KYC Review - For low risk NPS customers KYC review will be done after every 10 years as already prescribed in the KYC policy of the Bank.

ii. **Moderate Risk** – Customers opening Tier-1 NPS accounts on voluntary basis will be classified under moderate risk. As PFRDA has not defined any period for KYC review of moderate risk NPS Tier – 1 customers, we may treat "moderate risk" as "medium risk"

KYC Review - KYC review for medium risk NPS Tier- 1 customers will be done after every 8 years as per existing KYC policy of the bank.

iii. **High Risk -** For the high-risk profiles, like for subscribers(customers) 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.

Voluntary contributions towards NPS Tier II account, which is a withdrawable account involve generally higher risk in comparison to other categories. As such the customers opening NPS Tier-2 account will be classified under high risk category.

KYC Review - KYC review for high risk NPS Tier- 2 customers will be done after every 2 years as per existing KYC policy of the bank.

B. Existing subscribers/customers

The AML/CFT requirements are applicable for all the existing subscribers (customers). Hence, necessary CDD with KYC (as per extant PML Rules) shall be done for the existing subscribers (customers) from time-to-time on the basis of adequacy of the data previously obtained. Further, periodic updation

of KYC of NPS account shall be done as follows:

a. NPS Tier 1 account customers:

Risk categorization of all the existing low risk customers having NPS Tier-1 accounts should be changed to medium risk category and system will check and display pop-up message on the CBS screen regarding KYC status.
If KYC updation date is less than 8 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low risk to medium risk.

For **medium and high-risk customers**, risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before further NPS transaction, KYC is to be updated in CBS.

b. In case of NPS Tier II accounts (including Tier II Tax Saver Scheme as well as 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.

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.

c) CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:

(i) Commencement of an account-based relationship with the customer.
(ii) Carrying out any international money transfer operations for a person who is not an account holder of the Bank.
(iii) When there is a doubt about the authenticity or adequacy of the customer identification data (CID) it has obtained.
(iv) Selling third party products as agent, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than rupees fifty thousand.

(v) Carrying out transactions for a non-account based customer, that is a walk- in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
(vi) When Bank has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
(vii) It is to be ensured that introduction is not to be sought while opening accounts.

For the purpose of verifying the identity of customers/subscribers of NPS at the time of commencement of an account-based relationship, Bank will, at its option, rely on customer due diligence done by a third party, subject to the following conditions:

(i) Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
(ii) Adequate steps are taken by Bank to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
(iii) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
(iv) The third party shall not be based in a country or jurisdiction assessed as high risk.
(v) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

Reliance on third party KYC for NPS Subscribers

For the purposes of KYC norms under clause 8, while Bank as reporting entity is 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.

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

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

d) MONITORING OF TRANSACTIONS

Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

e) MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY BANK

(i) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Bank from time to time.

(ii) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc., of the Bank. Further, the periodicity of risk assessment exercise shall be annually.

(iii) Integrated Risk Management Division shall carry out the above said Risk Assessment exercise on annual basis. The outcome of the exercise shall be put up to the Risk Management Committee of the Board and should be available to competent authorities and self-regulating bodies. Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

(iv) The respective Process Owner Divisions will review the Controls related to KYC and AML existing / introduced in the area of their operations and its effectiveness in controlling the risk and minimizing data inconsistencies, if any and take corrective action. This process will be undertaken at least once a year. Special emphasis will be given on Risk

Based approach to KYC-AML – Key areas of concern- Outliers.

f) Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. Bank shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

2.4.2 COMPLIANCE OF KYC POLICY

(i) Compliance of KYC Policy of the Bank, as advised in RBI's Master Directions on KYC will be ensured as under: -

a) DESIGNATED DIRECTOR:

(i) An Executive Director on the Board to be nominated as "Designated Director", as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. Designated Director shall be nominated by the Board.

(ii) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(iii) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

(iv) In no case, the Principal Officer be nominated as the 'Designated Director'.

b) PRINCIPAL OFFICER:

(i) The Board has nominated Dy. General Manager, In-charge Centralized AML Cell as Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations.

(ii) 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.

(iii) The contact details name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

(iv) 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 30 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.

(v) Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

(vi) The Principal Officer will report to Designated Director through Chief General Manager, FRMD, who shall be the administrative head of Centralized AML Cell and will oversee the functioning of Centralized AML Cell as per PML Act/ KYC Policy.

(v) The Principal Officer will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.

(vi) 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

Government Business Department, General Banking Division, HO will be responsible for ensuring compliance under the law/regulations of PFRDA.

(ii) COMPLIANCE MECHANISM

A. Compliance of KYC Policy will be ensured through: -

(i) A senior officer in the rank of General Manager who will constitute as 'Senior Management' for the purpose of KYC compliance.

(ii) Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / Zonal Office / Circle Office level.

(iii) All HO Divisions to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities, etc.

(iv) Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Compliance Division, HO.

(v) Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to their Controlling Office. Concurrent / internal audit to also

ensure verification of compliance with KYC guidelines in system through system generated reports from EDW / CBS.

(vi) At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.

(vii) Bank, through Government Business Department, General Banking Division, HO submit certificate of compliances provided in Annexure of Master Direction of PFRDA along with submission of annual compliance certificate i.e. till 31st October of succeeding Financial Year.

B. It is to be ensured that decision-making functions of determining compliance with KYC norms are not outsourced by the bank.

C. PML Rules require all offices, Point of Presence – Service Providers (PoP-SP) of the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment should-

i. be documented;
ii. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
iii. be kept up to date; and
iv. be available to competent authorities and self-regulating bodies.

D. The implementation of KYC-AML guidelines by branches in letter and spirit, has to be ensured by Zonal Managers / Circle Heads and the same is to be checked during their visit to branches.

E. **Internal Control / Audit**

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

2.4.3 REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA

In terms of Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and in terms of Rule 7 thereof, the following reports shall be furnished to Financial Intelligence Unit-India as per guidelines prescribed by RBI / FIU/PFRDA as applicable and within the timelines specified.

(i) Cash Transaction Report [CTR].
(ii) Suspicious Transactions Report [STR]
(iii) Counterfeit Currency Report [CCR]
(iv) Non-Profit Organisations Transaction report [NTR]
(v) Cross-border Wire Transfer Report [CWTR]

Detailed Guidelines regarding reporting Requirements to FIU-India have been given in Operational Guidelines for KYC Policy. Reporting to PFRDA in respect of NPS to be ensured by the Government Business Department, General Banking Division, HO.

Indicative list of various types of indicators, i.e., customer behavior and risk-based transaction monitoring (RBTM), high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at Annexure-III of Operational Guidelines for KYC Policy.

2.4.4 OTHER ASPECTS

Other KYC / AML Guidelines to be followed while onboarding of customers/subscribers of NPS such as customer due diligence (CDD) procedure, identification of Beneficial Owner, periodic updation of KYC, transaction monitoring, etc., are given in Part-II Operational Guidelines of KYC Policy) such as: -

(i) CDD Procedure for Individuals, Sole Proprietary firms, Legal Entities
(ii) Identification of Beneficial Owner
(iii) On-going Due Diligence
(iv) Enhanced and Simplified Due Diligence Procedure
(v) Record Management
(vi) Internal Control System
(vii) Requirements / Obligations under International Agreements
(viii) Other Instructions
(ix) Standard Operating Procedure for National Pension System (NPS) KYC updation and Risk categorization.

2.5 AUTHORITY FOR APPROVING OPERATIONAL GUIDELINES

Audit Committee of Executives will approve/allow amendment in operational matters related to KYC and AML.

2.6 DISCLOSURE OF POLICY

This Policy is meant for internal use of staff and will also be displayed on the Bank's Public Website.

2.7 OWNERSHIP OF THE POLICY

KYC Cell, Data Privacy & Management Division, will be the owner division and shall be responsible for formulating / reviewing / periodic updation of the policy.

2.8 VALIDITY AND REVIEW OF THE POLICY

The policy shall remain valid for twelve months from the date of approval by the Board and shall be subject to annual review.

Further, Audit Committee of Executives is authorized to

a. incorporate any changes necessitated in the policy for the interim period up to the next review, due to regulatory pronouncements made during the validity period of the policy; and

b. to extend the validity of Policy (Part-I) for a period up to three months and the Board will be informed of such extension subsequently at the time of annual review.

2.9 REPORTING

Not Applicable

2.10 EXCLUSIONS

Any exclusions in the KYC Policy shall be approved by The Board.

(Part II-Operational Guidelines)

Operational Guidelines for
Know Your Customer (KYC) Policy

Division : Data Privacy & Management Division
Version : 2025_KYC_1.1

Guidelines Custodian

Division	Data Privacy & Management Division
Officer in-charge	General Manager
Guidelines Contact	kyc@pnb.co.in

Guidelines Version Control

S.N.	Version Number	Version Date	Summary of Changes
1	2023_KYC_1.0	01 March 2023	Periodic updation, Cash Transaction Report, Internal control system.
2	2023_KYC_1.1	11 May 2023	Guidelines updated as per RBI, Master Directions dated 28.04.2023 & 04.05.2023
3	2023_KYC_1.2	05 Oct 2023	Guidelines updated as per GOI, MOF Gazette Notification dated 04.09.2023
4	2023_KYC_1.3	01 Nov 2023	Guidelines updated as per RBI, Master Directions dated 17.10.2023
5	2024_KYC_1.0	06 Feb. 2024	Enhanced Due Diligence – Accounts of Politically exposed persons, Periodic Updation
6	2024_KYC_1.1	10 December 2024	PFRDA Master Direction on KYC for NPS as per PFRDA/Master Circular/2024/04/PoP-02 dated 23.01.2023 updated as on 10.04.2024
7	2025_KYC_1.0	19 March 2025	RBI updated its Master Direction – Know Your Customer (KYC) Direction, 2016 on updated 06.11.2024 and PFRDA updated its Master Direction on 23.09.2024.
8	2025_KYC_1.1		RBI updated its Master Direction – Know Your Customer Direction, 2016 on 12.06.2025.

Guidelines Governance

Frequency Of Review	Annual
Last reviewed on	04.01.2025
Approval Path	ACE
Supersedes	Data Privacy & Management Division Circular No. 13/2025 dated 19.03.2025

Operational Guidelines for KYC Policy

Part-II operational guidelines for KYC Policy describing definitions, customer due diligence procedure, record management, reporting requirements to FIU-IND, obligations under international agreements and other instructions are as under:

1. Definitions

In terms of RBI's Master Direction on KYC, unless the context otherwise requires, th terms herein shall bear the meanings assigned to them below:

(A) Terms bearing meaning assigned in terms of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005:

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

ii. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii. **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv. Beneficial Owner (BO)

a. **Where the customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has / have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of / entitlement to more than 10 per cent of the shares or capital or profits of the company.

(ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders'

agreements or voting agreements.

b. **Where the customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has / have ownership of / entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation-For the purpose of this clause, "Control" shall include the right to control the management or policy decision.

c. **Where the customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has / have ownership of/ entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. **Where the customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v **"Certified Copy of OVD"** - Obtaining a certified copy by bank shall mean comparing the copy of officially valid document so produced by the customer/subscribers of NPS with the original and recording the same on the copy by the authorized officer of the Branch under his GBPA/PF no. Branch Official will also attest the duly signed photograph of the customer, in the manner specified by RBI/PFRDA.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

A. Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
B. Branches of overseas banks with whom Indian banks have relationships,
C. Notary Public abroad,

D. Court Magistrate,
E. Judge,
F. Indian Embassy/Consulate General in the country where the non-resident customer resides.

vi. **"Central KYC Records Registry"** (CKYCR) means an entity defined under Rule 2(1) (aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vii. **"Designated Director"** means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

viii. **"Digital KYC"** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Bank as per the provisions contained in the Act.

ix. **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000). [Presently, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an *electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.]*

x. **"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 customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

[Presently, as per Information Technology Rules 2016, Rule 9 is related to the manner in which Digital locker System be used by issuer].

xi. "**Group"- The term "group"** shall have the same meaning assigned to it in clause (e) of sub section (9) of section 286 of the Income -tax Act,1961 (43 of 1961).

xii. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

xiii. **"Non-profit organisations"** (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of

section 2 of the Income-Tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

xiv. **"Officially valid document"** (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

Further, at the time of on-boarding of the customer, an undertaking should be obtained from the customer along with AOF/OVDs stating that Customer shall submit his OVD with updated current address within 3 months failing which operations in his account shall be restricted.

c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above, failing which the operations in the account shall be restricted (Debit-freezed).

d. Where the OVD presented by a foreign national does not contain the

details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xv. **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xvi. **"Person"** has the same meaning assigned in the Act and includes:

a. an Individual,
b. a Hindu undivided family,
c. a Company,
d. a Firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvii. "**Principal Officer (PO)**" means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules. Provided that such officer shall be an officer at the management level.

xviii. "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(i) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
(ii) appears to be made in circumstances of unusual or unjustified complexity; or
(iii) appears to not have economic rationale or bona-fide purpose; or
(iv) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to

terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

xix. **A 'Small Account'** means a savings account which is opened in terms of sub- rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 5.

xx. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of an account;
b. 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;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

xxi. "**UCIC"** means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

(B) Terms bearing meaning assigned in RBI Master Directions on KYC/Master Circular PFRDA, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. **"Common Reporting Standards"** (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters (MAAT).

ii. **Correspondent Banking:** Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

iii. **"Customer"** means a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iv. **"Walk-in Customer"** means a person who does not have an account based relationship with the Bank, but undertakes transactions with the Bank.

v. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
(c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

vi. **"Customer identification"** means undertaking the process of CDD.

vii. **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

viii. **"IGA"** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

ix. **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

x. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch / offices of the Bank or meeting the officials of Bank.

xi. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that those are consistent with the Bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

xii. **"Payable-through accounts":** The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

xiii. **"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 the Reserve Bank/PFRDA.

xiv. **"Shell Bank"** means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xv. **"Video based Customer Identification Process (V-CIP)"**: an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Bank by undertaking seamless, secure, live/real time with geo tagging, informed-consent based audio-visual interaction with the customer/subscribers to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face- to-face CIP for the purpose of this KYC Policy.

xvi. **"Wire transfer" related definitions:**

a. Batch transfer: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.

b. Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
c. Beneficiary Bank: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary Bank and makes the funds available to the beneficiary.
d. Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
e. Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
f. Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
g. Financial Institution: In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
h. Intermediary Bank: Intermediary Bank refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
i. Ordering Bank: Ordering Bank refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
j. Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or

legal person that places the order with the ordering financial institution to perform the wire transfer.

k. Serial Payment: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).

l. Straight-through Processing: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

m. Unique transaction reference number: Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

n. Wire transfer: Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

xvii. **"Point of Presence"** means an intermediary registered with the Authority under sub-section (3) of section 27 of PFRDA Act, 2013 as a point of presence and capable of electronic connectivity with the central recordkeeping agency for the purposes of receiving and transmitting funds and instructions and pay out of funds;

POP is the point of interaction between the subscriber and the NPS architecture. Point of Presence (POP) shall perform the functions related to registration of subscribers, undertaking Know Your Customer (KYC) verification, receiving contributions and instructions from subscribers and transmission of the same in the NPS architecture. POP(s) and their authorized branches (POP-SPs) shall also be required to comply with the provisions of the Prevention of Money Laundering (PML) Act, 2002 and the rules framed thereunder, as may be applicable, from time to time.

(C) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies,

Benefits and Services) Act, 2016, Pension Fund Regulatory and Development Authority Act, 2013, Unlawful Activities (Prevention) Act, 1967 and in all other regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

2. Customer Due Diligence (CDD) Procedure

2.1 CDD Procedure in case of Individuals

For undertaking CDD, concerned offices shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

a) the Aadhaar number where,
   i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
   ii. he decides to submit his Aadhaar number voluntarily to the bank; or
      (aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
      (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
      (ac) the KYC Identifier with an explicit consent to download records from CKYCR; and
b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, and
c) one recent photograph; and
d) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Bank:

Provided that where the customer has submitted,

i. Aadhaar number under clause (a) above, authentication of the customer's Aadhaar number to be carried out using e-KYC authentication facility provided by the Unique Identification Authority of India.

   Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository (CIDR), he may give a self-

declaration to that effect to the Bank.

ii. proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.

iii. an equivalent e-document of any OVD, the Bank 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 under Annexure II of Operational Guidelines for KYC Policy.

iv. any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Bank shall carry out verification through Digital KYC as specified under Annexure II of Operational Guidelines for KYC Policy.

v. KYC Identifier under clause (ac) above, the Bank shall retrieve the KYC records online from the CKYCR in accordance with Section 40.

Provided that for a period not beyond such date as may be notified by the Government for a class of Banks, instead of carrying out digital KYC, the Bank if pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, it shall be ensured that apart from obtaining the Aadhaar number, identification to be performed preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 2.4.2 (c) of Part-I Policy documents. It is to be ensured to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: Branch/Offices shall, where its customer submits his/her proof of possession of Aadhaar Number containing Aadhaar Number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators (BF).

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar, etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

While establishing an account based relationship with individual customer, the branch official to ascertain as to whether the customer is already having a Customer ID with the Bank. In case the customer has an existing Customer ID, fresh Customer ID shall not be created and the new account shall be opened with the existing Customer ID.

The name, father's name, date of birth and address of the customer be filled in the same manner and style as it appears in the KYC document provided by the customer. Branch official will ensure that all the mandatory fields in Account Opening Form / Customer Master Form (marked as *) such as Name, Father's name, date of birth, address, Identity Proof, address proof, Identification number (Identity proof document number), Profession / activity (Nature of Business - specific), total annual income, total annual turnover (in case of business), etc., are completely and correctly filled in by the customer and are also correctly captured in customer's database in CBS. The respective division/ offices of the Bank shall ensure that branches are capturing correct data in CBS system, particularly in respect of Constitution Code, Profession/ Activity, Occupation, Income/ Turnover, etc., as risk category of the customer is assigned on the basis of these parameters.

In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain. PAN Card and Voter Identity Card, wherever obtained, be verified on-line through the following websites and a print of on-line verification of the said document be held on record with the relevant AOF:

Name of Documents	Website / Link
PAN Card	Finacle Home Page > Non CBS Applications >GBD > On line PAN verification
Voter Identity Card	www.nvsp.in (National Voters Service Portal)

2.2 Client Due Diligence (CDD) for NPS Subscribers

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

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. Such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk clients.

2) Knowing existing subscribers

The AML/ CFT requirements are applicable for all the existing subscribers. Hence, necessary CDD with KYC (as per extant PML Rules) shall be done for the existing subscribers from time-to-time basis the adequacy of the data previously obtained.

3. **Accounts opened using Aadhaar OTP based e-KYC**, in non-face to face mode are subject to the following conditions:

(i) There must be a specific consent from the customer for authentication through OTP.
(ii) As a risk-mitigating measure for such accounts, it shall be ensured that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. There shall be a board approved policy in the Board delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
(iii) The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

(iv) The aggregate of all credits in a financial year, in all the deposit taken together,shall not exceed rupees two lakh.

(v) As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

(vi) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 2 or as per Section 4 (V-CIP) is carried out. If Aadhaar details are used under Section 4, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

(vii) If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

(viii) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non- face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

(ix) Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above-mentioned conditions.

4. Bank may undertake **Video based Customer Identification Process (V-CIP)** to carry out:

(i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 8 and Section 8A, apart from undertaking CDD of the proprietor.

(ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 3.

(iii) Updation/Periodic updation of KYC for eligible customers.

While undertaking V-CIP, following minimum standards have to be adhered to:

(A) V-CIP Infrastructure

(i) Adherence to RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third –party technology provider assisting the V-CIP of the Bank.

(ii) End-to-end encryption of data between customer device and the hosting point of the V-CIP application to be ensured, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

(vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-event under extant regulatory guidelines.

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical

gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(B) V-CIP Procedure

Concerned Division shall formulate a clear work flow and standard operating procedure for V-CIP and adherence to it should be ensured. Any modification in the work flow/SOP may be carried out only after approval from Operational Risk Management Committee (ORMC). The V-CIP process shall only be carried out by Bank officials specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

Concerned Division(s)/Designated Official(s) undertaking V-CIP shall ensure that:

(i) In case of, disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the concerned official. However, in case of call drop / disconnection, fresh session shall be initiated.

(ii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

(iii) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

(iv) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

(v) The authorized Bank official performing the V-CIP shall record audio-

video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a. OTP based Aadhaar e-KYC authentication.
b. Offline Verification of Aadhaar for identification.
c. KYC records downloaded from CKYCR, in accordance with section 40, using the KYC identifier provided by the customer.
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

It is to be ensured to redact or blackout the Aadhaar number in terms of Section 2.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, it is to be ensured that the video process of the V-CIP is undertaken within three working days of downloading /obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, it is to be ensured that no incremental risk is added due to this.

(vi) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

(vii) The authorised official of the bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi locker.

(viii) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(ix) The authorised official of the Bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by

the customer.

(x) Assisted V-CIP shall be permissible when bank take help of Banking Correspondents (BCs) facilitating the process only at the customer end. The details of the BC assisting the customer have to be maintained, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

(xi) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

(xii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank.

(C) V-CIP Records and Data Management

(i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this KYC Policy of the Bank, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the official performing the V- CIP shall be preserved.

5. Small Account

Notwithstanding anything contained in Section 2 and as an alternative thereto, in case an individual who desires to open a bank account, bank shall open a 'Small Account', which entails the following limitations:

(i) the aggregate of all credits in a financial year does not exceed rupees one lakh;

(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

(iii) the balance at any point of time does not exceed rupees fifty thousand.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

a) A self-attested photograph to be obtained from the customer.
b) The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
   Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
d) It is to be ensured that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
f) The entire relaxation provisions shall be reviewed after twenty-four months.
g) Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020and such other periods as may be notified by the Central Government.
h) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high-risk scenarios, the identity of the customer shall be established as per Section 2 or Section 4.
i) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 2 or Section 4.

6. Transfer of Account from one branch to another branch

KYC verification once done by one branch / office of the Bank shall be valid for transfer of the account to any other branch / office of the same Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

7. CDD Measures for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

8. Business/ Activity proof for Sole Proprietary firms

In addition to the above, any two of the following documents or the equivalent e-document thereof as a proof of business / activity in the name of the proprietary firm shall also be obtained:

(i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
(ii) Certificate / Licence issued by the municipal authorities under Shop andEstablishment Act.
(iii) Sales and income tax returns.
(iv) CST / VAT / GST certificate.

(v) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
(vi) IEC (Importer Exporter Code) issued to the proprietary concern by the officeof DGFT / Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
(vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities.
(viii) Utility bills such as electricity, water, and landline telephone bills.

8A. In cases where the concerned office is satisfied that it is not possible to furnish two such documents, the concerned office may, at their discretion, accept only one of those documents as proof of business / activity.

Provided it undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

CDD Measures for Legal Entities

9. For opening an account of a company, certified copies of each of the followingdocuments or the equivalent e-document thereof shall be obtained:
(i) Certificate of incorporation;

(ii) Memorandum and Articles of Association;
(iii) Permanent Account Number of the company;
(iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
(v) Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
(vi) the names of the relevant persons holding senior management position: and
(vii) the registered office and the principal place of its business, if it is different**.**

10. **For opening an account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    (i) Registration certificate;
    (ii) Partnership deed;
    (iii) Permanent Account Number of the partnership firm;
    (iv) Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
    (v) The names of all the partners; and
    (vi) address of the registered office, and the principal place of its business, if it is different.

11. **For opening an account of a trust,** certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    (i) Registration certificate;
    (ii) Trust deed;
    (iii) Permanent Account Number or Form No.60 of the trust;
    (iv) Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
    (v) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust;
    (vi) the address of the registered office of the trust; and
    (vii) list of trustees and documents, as are required for individuals under Section 2 for those discharging role as trustee and authorised to transact on behalf of the trust.

12. **For opening an account of an unincorporated association or a body of**

individuals, certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

(i) Resolution of the managing body of such association or body of individuals;
(ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
(iii) Power of attorney granted to transact on its behalf;
(iv) Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
(v) such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies.

13. **For opening account of a customer who is a juridical person (not specifically covered in the earlier part)** such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents there of shall be obtained and verified:

(i) Document showing name of the person authorised to act on behalf of the entity;
(ii) Documents, as specified in Section 2, of the person holding an attorney to transact on its behalf and
(iii) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

Provided that in case of a trust, it shall be ensured that trustees disclose their status at the time of commencement of an account based relationship or when carrying out transactions as specified in clauses (ii), (v) and (vi) of section 2.4.1 (c).

14. **For opening an account of Hindu Undivided Family,** certified copies of each of the following documents shall be obtained:

(i) Identification information as mentioned under Section 2 in respect of the Karta and Major Coparceners,

(ii) Declaration of HUF and its Karta,
(iii) Recent Passport photographs duly self-attested by major co-parceners alongwith their names and addresses.
(iv) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

15. Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficialowner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his / her identity shall be undertaken keeping in view the following:

a. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdiction notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

b. In cases of trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

16. On-going Due Diligence

On-going due diligence of customers to be undertaken to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds / wealth.

16.1 Ongoing Due Diligence for NPS Subscribers

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 Bank for further ongoing due diligence processes and action as considered necessary.

A. Bank as a Reporting entity shall identify the source of contribution and ensure that the contribution is being done through the subscriber's source of funds.

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

1. No payments should be made to third parties on attainment of superannuation except payments to nominee(s)/ legal heir(s) in case of death.

2. Necessary due diligence of the subscriber(s) / nominee(s) / legal heir(s) should be carried out before making the pay-outs/settling claims.

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

17. Types of transactions for monitoring

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- **a.** Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- **b.** Transactions which exceed the thresholds prescribed for specific categories of accounts.
- **c.** High account turnover inconsistent with the size of the balance maintained.
- **d.** Deposit of third party cheques, drafts, etc., in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, Bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

18. The extent of monitoring shall be aligned with the risk category of the customer

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

(b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND

19. Updation / Periodic Updation

A risk-based approach is adopted by the Bank for periodic updation of KYC. Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. (The detailed 'Standard Operating Procedure for Periodic KYC Updation' has been placed at Annexure-I of Operational Guidelines for KYC Policy). **Notwithstanding the provisions given above, in respect of an individual customer who is categorized as low risk, the bank shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The bank shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.**

a. Individual Customers:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter, etc. (Refer Annexure-I of Operational Guidelines for KYC Policy).

ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. (Refer Annexure-I of Operational Guidelines for KYC Policy).

ii(a). Use of Business Correspondent (BC) by bank for Updation/ Periodic Updation of KYC:

Self-declaration from the customer in case of no change in KYC information or change only in the address details may be obtained through an authorized BC of the bank. The bank shall enable its BC systems for recording these self-declarations and supporting documents thereof in electronic form in the bank's systems.

The bank shall obtain the self-declaration including the supporting documents, if required, in the electronic mode from the customer through the BC, after successful biometric based e-KYC authentication. Until an option is made available in the electronic mode, such declaration may be submitted in physical form by the customer. The BC shall authenticate the self-declaration and supporting documents submitted in person by the customer, and promptly forward the same to the concerned bank branch. The BC shall provide the customer an acknowledgment of receipt of such declaration /submission of documents.

The bank shall update the customer's KYC records and intimate the customer once the records get updated in the system, as required under paragraph 19 (c) of KYC Policyibid. It is, however, reiterated that the ultimate responsibility for periodic updation of KYC remains with the bank concerned.

iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the base branch. Wherever required, branch may carry out fresh KYC of such customers, i.e., customers for whom account was opened when

they were minor, on their becoming a major. As the KYC documents are to be maintained at base branch, the customer may contact his/her base branch or use V-CIP for updation.

iv. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 3 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Bank shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

v. Further, periodic updation of KYC of NPS account shall be done as follows:

NPS Tier 1 account customers:

Risk categorization of all the existing low risk customers having NPS Tier-1 accounts should be changed to medium risk category and system will check and display pop-up message on the CBS screen regarding KYC status.

If KYC updation date is less than 8 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low risk to medium risk.

For **medium and high-risk customers**, risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before further NPS transaction, KYC is to be updated in CBS.

a. In case of NPS Tier II accounts (including Tier II Tax Saver Scheme as well as Politically Exposed Person (PEP) - Every 2 years.
b. At the time of exit from NPS Tier I account.
c. Whenever there is upward revision in the risk profile of the subscriber.
d. As and when there are revision or changes in PML Act / PML Rules.

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

b. Customers other than individuals:

i. **No change in KYC information:** In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration (letter from an official authorized by the LE in this regard, board resolution, etc.) in this regard shall be obtained from the LE customer through its email id registered with the Bank/ by post/ by visiting the base branch. Further, branch shall ensure during this process that Beneficial Ownership (BO)/Authorised Signatories information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. **Change in KYC information:** In case of change in KYC information, Bank shall undertake the KYC process equivalent to that applicable for on- boarding a new LE customer.

c. Additional measures: In addition to the above, it shall be ensured by the concerned offices that,

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Bank has expired at the time of periodic updation of KYC, Bank shall undertake the KYC process equivalent to that applicable for on- boarding a new customer.

ii. Customer's PAN details, if available with the Bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out **updation / periodic updation**. Further, it shall be ensured that the information/ documents obtained from the customers at the time of **updation / periodic updation** of KYC are promptly updated in the records / database of the Bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

d. In case of existing business relationship which is not KYC compliant, customer induced debit operations in CASA and CC/OD accounts linked with that customer ID to be temporarily ceased. However, before temporarily ceasing operations for an account, it is to be ensured to give

the client two notices of 10 days each and within 30 days period the account should be made KYC compliant otherwise customer induced debit operations in CASA and CC/OD accounts linked with that customer ID shall be frozen. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

e. Bank shall advise the customers that in order to comply with the PML rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.

f. Due Notices for Periodic Updation of KYC: **The bank shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the bank shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the bank shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the bank's system against each customer for audit trail.**

20. Freezing and closure of Non- KYC Compliant Accounts

In case of existing customers, the Permanent Account Number or the equivalent e- document thereof or Form No.60 to be obtained, by such date as may be notified by the Central Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or the equivalent e- document thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the client

is to be given an accessible notice and a reasonable opportunity to be heard. However, operations in accounts of customers who are unable to provide Permanent Account Number or the equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes, may allowed to be continued. The Branch Head shall allow such relaxation for continuation of operations in such accounts till the time PAN or the equivalent e-document thereof or Form 60 is obtained from the customer for which an officer from the branch will be deputed to personally visit the customer for obtaining the PAN or the equivalent e-document thereof or Form 60. However, the Branch Head shall ensure that such accounts are subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Bank gives in writing to the Bank that he does not want to submit his Permanent Account Number or the equivalent e-document thereof or Form No.60, Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation — For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence (EDD)

21. Enhanced Due Diligence (EDD) for non-face-to-face customer on-boarding (other than customer on-boarding in terms of Section 3): Non-face-to-face on-boarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by REs for non-face-to-face customer on-boarding (other than customer on-boarding in terms of Section 3):

a) In case Bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote on-boarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this KYC Policy.
b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Bank shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
c) Apart from obtaining the current address proof, concerned official shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
d) PAN shall be obtained from the customer and it shall be verified from the verification facility of the issuing authority.
e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

22. Accounts of Politically Exposed Persons (PEPs)

a. The Branch / Offices shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

(i) It shall be ensured by branch/offices that risk has been assigned as per Bank guidelines where the customer or the beneficial owner is a PEP.
(ii) Reasonable measures are taken for establishing the source of funds / wealth;
(iii) the approval to open an account for a PEP shall be obtained from the senior management, i.e., at the level of Chief manager and above, in accordance with the Bank' Customer Acceptance Policy;
(iv) all such accounts are subjected to enhanced monitoring on an on-going basis;
(v) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval, i.e., Chief Manager and above is obtained to continue the business relationship;

b. These instructions shall also be applicable to family members or close associates of PEPs.

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

22 A. Pension accounts of Politically Exposed Persons (PEPs)

The customer due diligence guidelines as per existing KYC Policy of the Bank for Politically Exposed Persons (PEPs) will be also applicable to their Pension accounts.

Bank 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.

23. Client accounts opened by professional intermediaries:

While opening client accounts through professional intermediaries, it is to be ensured that:

a. Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b. Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c. Accounts of such professional intermediaries not to be opened, who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
d. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the concerned office shall look for the beneficial owners.
e. The offices shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
f. The ultimate responsibility for knowing the customer lies with the Bank.

23A. Identification and monitoring of Money Mule Accounts

a. Accounts of natural persons having very low balance (say a few hundred rupees) and not operated for more than a year

OR

b. Accounts of natural persons having been opened as small accounts, as defined in Section 5 of Operational Guidelines of KYC policy.

AND

c. Receiving multiple credits of small amounts in quick succession in a very short span of time followed by immediate withdrawals (cash or transfer, single or multiple) would be flagged as suspected money mule accounts.

Any such account, which has been flagged as suspected money mule account, would immediately be subjected to Enhanced Due Diligence (EDD) and enhanced monitoring without any tip off to the customer. The accounts then identified as suspected money mule shall be reported in Suspicious Transaction Report (STR) to FIU-IND by CAML Cell.

B. Simplified Due Diligence

24. Simplified norms for Self Help Groups (SHGs)

a. CDD of all the members of SHG shall not be required while opening savings bank account of SHG.
b. CDD of all the office bearers shall suffice.
c. Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

25. Procedure to be followed by the offices while opening accounts of foreign students

a. The offices shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
   (i) Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.
   (ii) Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

b. The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA. 1999.
c. Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

26. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible / registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annexure-IV of operational Guidelines for KYC Policy, subject to Income Tax (FATCA / CRS) Rules.

Provided that offices shall obtain undertaking from FPIs or the Global Custodian

acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annexure-IV of Operational Guidelines for KYC Policy will be submitted.

27. Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. It is to be ensured to,

a. maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction;

b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

c. make available swiftly, the identification records and transaction data to the competent authorities upon request;

d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

e. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, includingthe following:

(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it was denominated;
(iii) the date on which the transaction was conducted; and
(iv) the parties to the transaction.

f. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

g. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation-For the purpose of this Section, the expressions "records pertaining to the identification", "Identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any

analysis undertaken.

27A. Bank shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

For the existing NPO customers, the Bank may follow up with such NPO customers for getting them registered on DARPAN portal, if not already done.

28. Reporting Requirements to Financial Intelligence Unit – India

In addition to above, every reporting entity should register with Financial Intelligence Unit - India (FIU-IND) under the regulator "PFRDA", and shall also furnish to the Director, Financial Intelligence Unit- India (FIU-IND), information referred to in Rule 3 (Maintenance of records of transactions (nature and value)) in terms of Rule 7 (Procedure and manner of furnishing information) of the PML (Maintenance of Records) Rules, 2005.

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.

29. The Reporting Formats

The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Bank 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 Bank which are yet to install/adopt suitable technological tools for extracting CTR / STR from their live transaction data.

30. Furnishing of Information

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. Branch/offices shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

Bank, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 2.3.2 of Part-I Policy of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

31. Robust software,

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

Bank 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.

Bank 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.

32. Reports to be furnished to Financial Intelligence Unit-India

(1) Cash Transactions Report [CTR]

(i) Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh.

(ii) The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

(iii) A copy of monthly CTR submitted on its behalf to FIU-IND is available at

the concerned branch (through MIS Report: Misc Reports Module under SENSRPT — 5/7 & 5/7a) for production to auditors/Inspectors, when asked for.

(2) Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, bank is to be guided by the definition of "suspicious transaction" as contained in PMLA Rules as amended from time to time.
"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

(ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted transactions in STRs to be reported, even if not completed by the customers, irrespective of the amount of the transaction.
(iii) STR to be submitted if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
(iv) Furnishing of STR to be ensured within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

(v) It shall be ensured not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that thereis no tipping off to the customer at any level.

(vi) The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular.

(vii) For effective monitoring of transactions of the customers, Bank has implemented an AML system for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. Further, an indicative list of behavioral /observation based scenarios has been circulated vide Centralised AML Cell (FRMD) Circular No. 01/2021 dated 22.01.2021. In case any suspicious transaction is detected, the same be reported to Centralised AML Cell for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FIN net Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators, i.e., customer behavior and risk based transaction monitoring (RBTM), high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at **Annexure-lll** of Operational Guidelines for KYC Policy.

(3) Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.

(4) Non Profit Organisations Transaction report [NTR]

All transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency, to be reported to the Director, Financial Intelligence Unit-India by the 15th of the succeeding

month.

(5) Cross-border Wire Transfer Report [CWTR]

Cross-Border Wire Transfer Report (CWTR) to be filed to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs. 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

(6) Additional measures

(a) Charted Accountants, Company Secretaries and Cost and Works Accountants practicing individually or through a firm shall report suspicious transactions when, on behalf of his client, they engage in a financial transaction in relation to the following activities: -

(i) buying and selling of any immovable property;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) organization of contributions for the creation, operation or management of companies;

(v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities;

(b) Any individual performing the following activities when carried out in the course of business on behalf of or for another person shall report suspicious transactions: -

(i) acting as a formation agent of companies and limited liability partnerships;

(ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a firm or a similar position in relation to other companies and limited liability partnerships;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company or a limited liability partnership or a trust;

(iv) acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another type of trust; and

(v) acting as (or arranging for another person to act as) a nominee share holder for another person;

32A Implementation of group-wide policy-

As per Section 2.3.2 of Part-I Policy, the group shall discharge obligations under provisions of chapter IV of PMLA 2002 (15 of 2003).

The guidelines under this section apply to the group to the extent these are not contradictory to the local laws in the host country, provided that-

Where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India. In case there is a variance in KYC / AML standards prescribed by the Reserve Bank of India and the host country regulators, branches / overseas subsidiaries of Bank are required to adopt the more stringent regulation of the two.

Implementation of guidelines under this Section shall be ensured as under-

(i) These guidelines shall form part of KYC Policy of the group.
(ii) Independent evaluation of the compliance functions of above guidelines shall be ensured.
(iii) Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to their Controlling Office.
(iv) Half-yearly confirmation of implementation of above guidelines shall be submitted by foreign branches and majority owned subsidiaries through Group Business Management Division (GBMD) and Regional Rural Banks (RRBs) through Financial Inclusion (FI) Division of the Bank to KYC Section, Operations Division.

33. Internal Control System

(i) One Nodal officer at each Circle Office (Scale IV) & Zonal Office (Scale V) has been designated for compliance of KYC Policy and to monitor and strengthen the internal control system for prevention of money laundering and combating financing of terrorism.

The Nodal Officers will ensure compliance of the following aspects:

a. To comply with obligations under Prevention of Money Laundering Act / Rules, 2002 / 2005.

b. To comply with other related Laws / Ordinances / Instructions / Guidelines issued by the different Competent Authorities for prevention of money laundering and combating financing of terrorism.
c. To ensure that banking channel / products / services are not misutilized for money laundering to the detriment of national interest.
d. To submit STRs for the instances surfacing in local adverse media reports, enquiries conducted by Law Enforcement Agencies, public complaints, behavioural scenarios and attempted transactions, etc., to Centralized AML Cell, Faridabad at caml@pnb.co.in in compliance of the CAML (FRMD) Circular No. 01/2021 dated 22.01.2021 and CAML (FRMD) Circular No. 05/2022 dated 08.04.2022 besides other relevant circulars issued from time to time.
e. To ensure that field functionaries under their command area are sensitized on KYC / AML guidelines and ensuring that no money laundering activities take place in the branches under their jurisdiction.
f. To undertake on-site supervision by visiting the branches under their jurisdiction for random checking of compliance of KYC / AML guidelines of the Bank.

(ii) Centralized AML Cell:

Makers at Centralized AML Cell will analyse the alerts pertaining to their assigned areas (like Zones / Circles / Scenarios / Alert Frequency, etc.) on day to day basis and escalate to the Checker for closure or further necessary action. Checkers will check the action of the maker and after thorough analysis of the transactions /alerts, will close the alerts after ensuring that all the transactions are genuine in nature and match with the business profile of the customer, escalate for further action or reassign to the maker for further analysis in case any further information is required.

Post-closure scrutiny of closed alerts (@20%) shall be undertaken at Centralised AML Cell by Officers upto Scale III.

Further, Chief Managers at Centralised AML Cell will also review / scrutinise atleast 5 % of the closed alerts, pertaining to their respective areas, on random sample basis. They will also ensure that necessary corrective steps are taken.

(iii) Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members. Senior Officers from the Zonal / Circle Offices, during their visits to the branches will ensure that KYC / AML guidelines are being strictly adhered to as per the laid down

procedures, keeping in view the risk involved in a transaction, account or banking/business relationship.

(iv) For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer identification data (CID) and other Customer Due Diligence information, transaction records and other relevant information.

(v) Audit Committee of Executives will allow amendment in operational matters related to KYC and AML.

(v) Whitelisting of Customers / Accounts from Generation of AML Alerts will be considered for Customers / Accounts relating to Central Government, State Government, Banks, Public Sector Undertakings, ATM Cash Replenishing Agencies engaged by the Bank for the purpose of ATM Cash Replenishment in the Bank, Account of Subsidiaries of the Bank and RRBs sponsored by the Bank. However, the alerts generated and auto closed due to whitelisting, will be available at Backend for analysis as and when required.

Requirements / Obligations under International Agreements- Communications from International Agencies

34. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

All offices shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals / entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated. xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

(b) The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated. xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

All offices shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by all the offices for meticulous compliance.

35. Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 **(Annexure-II of Master Direction of RBI on KYC as amended from time to time**).

35A Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated February 2, 2021 (**Annexure-II of Master Direction of RBI on KYC as amended from time to time**) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

(a) All offices shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (**Annexure III of Master Direction of RBI on KYC as amended from time to time).**

(b) In accordance with paragraph 3 of the aforementioned Order, all offices shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, all offices shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) In case of match in the above cases, the transaction details with full particulars of the funds, financial assets or economic resources involved, be immediately reported Centralised AML (CAML) Cell for onward submission of same to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent by the CAML Cell to State Nodal Officer, where the account / transaction is held and to the RBI.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) All offices may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the concerned office shall prevent such individual/entity from conducting financial transactions and immediately inform to CAML Cell for their onward intimating the same to the CNO by email, FAX and by post, without delay.

(g) In case an order to freeze assets under Section 12A is received by the Bank from the CNO, the Bank shall, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall immediately be forwarded by the concerned office to CAML Cell with full details of the asset frozen, as given by the applicant, for their onward submission of the same to the CNO by email, FAX and by post, within two working days.

37. All offices shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

37A. In addition to the above, all offices shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

37B. CAML Cell shall undertake counter measures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

38. Jurisdictions that do not or insufficiently apply the FATF Recommendations

a. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Enhanced due diligence measures shall be applied which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

b. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 38 a & b do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

c. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank / other relevant authorities, on request.

38A. Banks are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanction requirements.

Other Instructions

39. Secrecy Obligations and Sharing of Information:

a. All offices shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
b. While considering the requests for data / information from Government and other agencies, all offices shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
c. The exceptions to the said rule shall be as under:-
   i. Where disclosure is under compulsion of law,
   ii. Where there is a duty to the public to disclose,
   iii. the interest of bank requires disclosure and
   iv. Where the disclosure is made with the express or implied consent of thecustomer.
d. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer

39A. Compliance with the provisions of Foreign Contribution (regulation) Act, 2010.

International Banking Division (IBD) shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, meticulous compliance shall also be ensured with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India

40. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

a. Government of India has authorized the Central Registry of Securitization 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.
b. In terms of provision of Rule 9(1A) of PML Rules, the Bank has to capture customer's KYC records and upload onto CKYCR within 10

days of commencement of an account-based relationship with the customer.

c. Operational Guidelines for uploading the KYC data have been released by CERSAI.
d. All offices shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
e. The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, concerned offices are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. Bank was initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017.
f. KYC records pertaining to accounts of LEs opened on or after April 1, 2021 have to be uploaded, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.
g. Once KYC Identifier is generated by CKYCR, it is to be ensured that the same is communicated to the individual/LE as the case may be.
h. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updation as specified in paragraph 19 of the Policy, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Bank obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an Bank regarding an update in the KYC record of an existing customer, the Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank.
i. It is to be ensured that during periodic updation, the customers are

migrated to the current CDD standard.

j. For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

   i. there is a change in the information of the customer as existing in the records of CKYCR; or
   ii. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
   iii. The validity period of downloaded documents has lapsed; or
   iv. The Bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

The Reporting entities are required to perform the CKYCR related functions **such as filing, retrieval, and utilization of the KYC records with the Central KYC Records Registry or any other matter in connection with or incidental thereto**, in the manner as prescribed under the PML Rules. For the purpose of performing such functions the Banks are required to get registered 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, Banks already registered with CERSAI under another financial sector regulator are not required to register themselves with CERSAI again, and may use such **existing registration with CERSAI, for the purpose of fulfilling the obligations under the PFRDA Act and Regulations and these guidelines.**

l. For the purpose of verification of identity of a client **(Para 2.2)** or on-going due diligence (**Para 16.1),** the reporting entity shall seek the KYC Identifier from the client or retrieve the KYC Identifier, if available, from the Central KYC Records Registry and proceed to obtain KYC records online by using such KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless –

a) there is a change in the information of the client as existing in the records of Central KYC Records Registry;

or

b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the Authority;

or

c) the validity period of the downloaded documents has lapsed;

or

d) the reporting entity considers it necessary in order to verify the identity or address (including current address) of the client as per these guidelines, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

In terms of the provisions of Prevention of Money Laundering Act, 2002 9PML Act), Section 11A thereof and the Prevention of Money Laundering (Maintenance of records) Rules, 2005 (PML Rules), reporting entities (Bank) 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 an on-going basis.

These Guidelines are for use by PoPs, NPS Trust, CRAs and Retirement Advisers registered under the PFRDA Act and the respective Regulations.

II. A) A Reporting Entity after obtaining additional or updated information from the client during verification of identity of a client (**Para 2.2)** or On-going due diligence (**Para 16.1)** within seven (7) days or within such period as may be notified by the Central Government, furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client.

B). If any update in the KYC record of an existing client is received by reporting entity from Central KYC Records Registry as per Para 40(II) A, the Bank shall retrieve the updated KYC records from the Central KYC Records Registry and shall update the KYC record maintained by the reporting entity.

41. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, all offices shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

a. Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login → My Account → Register as Reporting Financial Institution,

b. Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: All offices shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

c. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

d. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

e. Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

f. Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. All offices may take note of the following:

i. updated Guidance Note on FATCA and CRS

ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

42. Period for presenting payment instruments

Payment of cheques / drafts / pay orders / banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

43. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." CAML Cell shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed, it shall then be deemed that these instructions have not complied with.

44.Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected.

45. Unique Customer Identification Code (UCIC)

a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by bank.
b) It is to be ensured not to issue UCIC to all walk-in / occasional customers. However, UCIC shall be allotted to such walk-in customers who have frequent transactions.

46.Introduction of New Technologies

Identification and assessment of ML/FT risk shall be done by the Bank that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, Bank shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

47.Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc.

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent banking and other similar relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

a. Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.
b. The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.
c. Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.
d. Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.

e. In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts of the correspondent bank and is undertaking on-going 'due diligence' on them.
f. The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.
g. Correspondent relationship shall not be entered into or continued with a shell bank.
h. It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.
i. Banks shall be cautious of correspondent banking relationships with institutions located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
j. Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

48.Wire transfer

All offices shall ensure the following while effecting wire transfer: -

A. Information requirements for wire transfers for the purpose of Operational Guidelines of KYC Policy

(i) All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a. name of the originator;
b. the originator account number where such an account is used to process the transaction;
c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
d. name of the beneficiary; and
e. the beneficiary account number where such an account is used to process the transaction.

In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

(ii) In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission

to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

(iii) Domestic wire transfer, where the originator is an account holder of the ordering Bank, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

(iv) Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering Bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering Bank and where the information accompanying the wire transfer can be made available to the beneficiary Bank and appropriate authorities by other means, it is sufficient for the ordering Bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.
The ordering Bank shall make the information available within three working/business days of receiving the request from the intermediary Bank, beneficiary Bank, or from appropriate competent authorities**.**

(v) All offices shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting /competent authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

(vi) The wire transfer instructions are not intended to cover the following types of payments:

a. Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a

payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

b. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the obligation of an office to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

B. Responsibilities of Ordering Bank, Intermediary Bank and Beneficiary Bank, effecting wire transfer, are as under:

(i) Ordering Bank:

a. The ordering Bank shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.
b. Customer Identification shall be made if a customer, who is not an account holder of the ordering Bank, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.
c. Ordering Bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this section.

(ii) Intermediary Bank:

a. Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.
b. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary Bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary Bank.

c. Intermediary Bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.
d. Intermediary Bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

(iii) Beneficiary Bank:

a. Beneficiary Bank shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.
b. Beneficiary Bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

(iv) Money Transfer Service Scheme (MTSS) providers and Bank are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. Banks that control both the ordering and the beneficiary side of a wire transfer shall: -

a. into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
b. file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

Other Obligations

(i) Obligations in respect of Bank's engagement or involvement with unregulated entities in the process of wire transfer

All offices shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned Bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,

i. there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
ii. the agreement / arrangement, if any, with such unregulated entities by Bank clearly stipulates the obligations under wire transfer instructions; and
iii. a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

(ii) Bank's responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)

All offices are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, all offices shall ensure that they do not process cross-border transactions of designated persons and entities.

(iii) Banks' responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the concerned office involved in the wire transfer, in accordance with Section 27 of Operational Guidelines of KYC Policy.

(iv) Responsibility of reporting entities as per PFRDA Guidelines for NPS

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

a. 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;
b. Reporting entities shall initiate appropriate actions against defaulting representative of reporting entity who expose the reporting entities to KYC / AML / CFT related risks.

As some reporting entities are allowed to engage the services of individuals like Retirement advisers and Pension 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.

Regulation 44 (2) of PFRDA (PoP) Regulations, 2018 as amended, specifies that "A point of presence shall be liable for any acts of omission or commission, by the pension agents in discharge of its functions, arising out of such engagement, including compliance with KYC and AML norms prescribed under Prevention of Money Laundering Act, 2002, monitoring and supervising their activities, imparting training on pension schemes to them.

c. Financial groups shall be required to implement group-wide programmes against ML / TF, which should be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group policies and procedures for sharing information required for the purposes of Customer Due Diligence and ML / TF risk management;

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

The overseas branches of the reporting entity to conduct client due diligence / AML standard for the subscribers specified by the PFRDA for the pension scheme regulated / administered by PFRDA. If the host country does not permit implementation of these guidelines, reporting entity should apply appropriate

additional measures to manage the money laundering and terrorist financing risks, and inform the same to PFRDA.

49. Issue and Payment of Demand Drafts, etc.

Any remittance of funds by way of demand draft, mail / telegraphic transfer / NEFT/ IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

50. Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time.Form 60 shall be obtained from persons who do not have PAN or equivalent e- document thereof.

51. Selling Third party products

Bank acting as agents while selling third party products as per regulations in force from time to time has to comply with the following aspects for the purpose of these directions:

a. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 2.4.1(c) of this Directions.
b. transaction details of sale of third party products and related records shall be maintained as prescribed in Section 27.
c. AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
d. transactions involving rupees fifty thousand and above shall be undertaken only by:
    i. debit to customers' account or against cheques; and
    ii. obtaining and verifying the PAN given by the account based as well as walk- in customers.
e. Instruction at 'd' above shall also apply to sale of Bank's own products,

payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for rupees fifty thousand and above.

52. At-par cheque facility availed by co-operative banks

a. The 'at par' cheque facility offered by Bank to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising there from.
b. The right to verify the records maintained by the customer cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by Bank.

53. Issuance of Prepaid Payment Instruments (PPIs):

It is to be ensured that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

54. Hiring of Employees and Employee training

a. Adequate screening mechanism, including Know Your Employee / Staff Policy, as an integral part of their personnelrecruitment/ hiring process shall be put in place.
b. Bank shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Bank shall also strive to develop an environment which fosters open communication and high integraty amongst the staff.

c. On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML / CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers/subscribers. The front desk staff shall be specially trained to handle issues arising from lack of customer/subscribers education. Proper staffing of the audit function with persons adequately trained and well-versed in AML / CFT policies of the Bank, regulation and related issues shall be ensured.

d. Ensure that the content of these guidelines are understood by all employees, associated Retirement Advisers and **Pension 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.

55. Validity and Review of the Operational Guidelines

The Operational Guidelines shall remain valid for twelve months from the date of approval of Policy (Part-I) by the Board and shall be subject to annual review.

Further, the Audit Committee of Executives is authorized to extend the validity of Operational guidelines (Part-II) for a period up to three Months and the Board will be informed of such extension subsequently at the time of annual review.

Annexure-I

STANDARD OPERATING PROCEDURE FOR PERIODIC KYC UPDATION

1. CHANNELS FOR PERIODIC KYC UPDATION OF INDIVIDUALS

1.1. Email-Id registered with the Bank/ By Post/ By Letter/ By visiting Branch

1.1.1. **No change in Customer Information-**

At Base Branch

a) For such cases, a customer can submit a self-declaration stating that there is no change in his/her KYC information to the Base Branch through email-id registered with the Bank/ by post/ by letter/ by visiting base branch.

b) Branch on obtaining the request from the Customer shall ascertain that KYC documents as per the current CDD standards are available with them and shall update the KYC status and KYC updation date in CBS. The Branch shall also upload the documents/details at CKYCR portal in terms of extant guidelines; where CKYC not yet done.

c) If the available documents, are not as per extant KYC policy or the OVD submitted by Customer has expired, the Branch shall inform the Customer to submit the requisite documents as per current CDD standard for KYC Updation.

d) The KYC documents/self-declaration obtained from customer shall be maintained alongwith Account Opening Form/Customer Master Form at the Base branch.

e) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

At Non Base Branch

a) For such cases, a customer to submit a self-declaration, along with KYC Updation form stating that there is no change in his/her KYC information by visiting any branch.

b) Branch on obtaining the request/self-declaration and KYC Updation form, from the customer, shall ascertain the identity/genuineness of the Customer by observing due diligence like matching photo/signature details available in CBS and further to ensure that KYC details available in CBS is as per current CDD standard of KYC Policy of the Bank.

c) Branch shall update the KYC status and KYC Updation in CBS

promptly.

d) Branch shall send duly authenticated original copy of self-declaration/request received from the customer to the Base Branch and retain duly authenticated copy of the same as per extant record maintenance policy of the Bank.

e) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

Responsibility of Base Branch:-

a) Branch upon receipt of self-declaration/request of the customer along with KYC upodation form, from the KYC updating branch, shall ensure that these documents are kept along with the AOF/ Customer Mater form maintained at the branch.

b) Branch shall ensure to upload the documents/KYC details at CKYCR portal in terms of extant guidelines; where CKYC not yet done.

1.1.2. Change in Address:

i. For cases where Customer is submitting KYC documents as per current CDD standards

At Base Branch: -

a) For such cases, the Customer shall submit KYC documents as per the current CDD standards to the Base Branch through email-id registered with the Bank/ by post/ by letter/ by visiting base branch.

b) Branch on obtaining the request from the Customer shall update the KYC details and KYC Updation date in CBS promptly. Further, branch shall also scan the KYC documents for CKYCR and upload the KYC documents/details at CKYCR portal in terms of extant guidelines.

c) The KYC documents/self-declaration obtained from customer shall be maintained along with Account Opening Form/Customer Master Form at the Base branch.

d) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

At Non -Base Branch: -

a) For such cases, the Customer shall submit KYC documents as per the current CDD standards by visiting at any branch.

b) Branch on obtaining the KYC documents and KYC Updation form Customer shall update the KYC details and KYC Updation date in CBS Promptly.

c) Branch shall send duly authenticated KYC documents/records received from the customer to the Base Branch and retain duly authenticated copies of the same as per extant record maintenance policy of the Bank.

d) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

Responsibility of Base Branch: -

a) Branch upon receipt of KYC records/documents of the customer, shall ensure that these documents are kept along with the AOF/ Customer Master form maintained at the branch.

b) Branch shall ensure to upload the documents/ KYC details at CKYCR portal in terms of extant guidelines; where CKYC not yet done

ii For cases where Customer is submitting a self-declaration of the new address

a) If a customer submits a self-declaration of the new address to the base branch, the same may be obtained from the customer through email-id registered with the Bank/ by post/ by letter/ by visiting base branch.

b) The base branch on obtaining the request shall ascertain that KYC documents as per the current CDD standards are available with them. If the available documents, are not as per extant KYC policy or the OVD submitted by Customer has expired, the Branch shall inform the Customer to submit the requisite documents as per current CDD standards for KYC Updation.

c) A menu option has been customized to capture the new address declared by customer. Both the existing & new address shall be maintained through this menu option.

d) On submission/verification by branch officials, the address shall be updated in CRM.

e) The branch shall verify the address by a positive confirmation within 30 days, by means such as address verification letter, contact point verification (CPV) by branch official. The confirmation process needs to be completed within 30 days from the updation date in CBS. In exceptional eventualities, period of positive confirmation may be

extended by controlling office for a maximum further period of 30 days as per procedure presently issued vide Operations Division (KYC Section) Circular No. 07/2023 dated 19.06.2023 and further as may be updated from time to time.

f) Upon successful confirmation, the Branch shall update the date of visit/letter in the newly customized menu option. The CBS shall update the flag for the positive confirmation. Further, branch shall also scan the KYC documents for CKYCR and upload the KYC documents/details at CKYCR portal in terms of extant guidelines.

g) If any verification fails through CPV/letter returns, the Branch shall update the same in the newly customized menu option (updating the status as confirmation failed). On updation, the previous address shall again be updated in the CRM and status quo shall be maintained in CBS/CRM. In such cases, the branch shall inform the Customer about failure in address verification requesting him/her to contact the branch for updation or use other channels for KYC updation. Further, system generated SMS shall also be sent to Customer on his registered mobile no. informing that Contact Point Verification of the declared address has failed and customer shall be requested to contact his/her base branch or use other channels for KYC updation.

h) The KYC documents/self-declaration and visit report/copy of address verification letter shall be maintained along with Account Opening Form/Customer Master Form at the Base branch.

i) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

1.2. <u>e-KYC authentication at any Branch</u>

i. Customers who are willing to undertake e-KYC authentication, may get their KYC Updated at any branch by submitting self-declaration for no change in ID/ address details OR any change in address by a self-declaration of the new address, to the Branch, while undertaking e-KYC.

ii. Upon successful e-KYC, the Branch shall update the KYC details through CCBM/CRM. The Branch shall maintain the record as per Record Maintenance Policy of the Bank.

iii. For such records, ITD will customize a mechanism for centralized uploading of KYC records/details at CKYCR, as is being done in case of new accounts opened with e-KYC.

iv. An acknowledgement of successful KYC updation shall be sent to

Customer on his/her registered mobile no. through SMS.

1.3. **Mobile No. registered with the Bank** (Only for no change in customer information)

i. The customer shall submit an SMS in the format **"KYCNC_Customer-ID"** from his registered mobile no. with the Bank to 5607040.
ii. The vendor handling the SMS functionality for the Bank, shall submit the SMS/information on real-time basis through API/web services or in batch mode at the end of day, to CBS for further processing.
iii. The CBS shall check whether the valid OVD (the 6 OVDs, as defined in KYC Policy) and Tax Proof (PAN/Form-60) are available for the said Customer-ID in CBS. Further, CBS shall also validate for any garbage/dummy data in OVD/Tax Proof. If any of above validations fails, an SMS shall be sent to Customer to contact Base Branch for KYC Updation.
iv. If the request clears the above validations, CBS shall update the KYC updation date in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.
v. For such records, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.

1.4. **PNB ATMs** (Only for no change in customer information)

i. The customer shall insert his debit card linked to Customer-ID in ATM and enter his 4-digit ATM PIN for verification. On successful verification of the PIN, Customer shall be provided an option for KYC Updation in Service Tab.
ii. On selecting the KYC Updation option, a new screen shall be displayed having following two options

   a) **Option 1:** If no change in customer information, then click submit
   b) **Option 2:** Otherwise press Cancel and please use other channels for submitting your latest KYC documents or contact your branch.

iii. If 'Option 1' is selected, ATM server shall retrieve all the linked Customer- IDs with the account and Customer shall be given the option to select the Customer-ID for KYC Updation is to be carried out. (Since ATM Card is linked with an account, there may be instances of it being a Joint Account, therefore the Customer shall

be provided an option to select the appropriate Customer-ID).

iv. After the Customer selects the requisite Customer-ID where KYC Updation is required to be carried out, the ATM server shall submit SMS/information on real-time basis through API/web services or in batch mode at the end of day, to CBS for further processing.

v. The CBS team shall check whether the valid OVD (the 6 OVDs, as defined in KYC Policy) and Tax Proof (PAN/Form-60) are available for the said Customer-ID in CBS. Further, CBS shall also validate for any garbage/dummy data in OVD/Tax Proof. If any of above validations fails, an SMS shall be sent to Customer to contact Base Branch for KYC Updation.

vi. If the request clears the above validations, CBS shall update the KYC updation date in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

vii. For such records, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.

1.5. Internet Banking/ Mobile Application (PNB ONE) of the Bank

i. The IBS/PNB ONE is operated at the Customer-ID Level.

ii. The Customer shall login in his internet banking/PNB ONE and will opt for option 'View Personal Information'. On selection, IBS/App shall retrieve and display KYC information to the Customer, such as Name, Father's Name, Mother's Name, Address, Annual Income, OVD Name & Number, OVD expiry date (in case of Passport & Driving License), Tax Proof Name & Number, Threshold Limit, Date of Birth, etc.

iii. If the OVD and Tax Proof submitted by the Customer in the Bank is not as per current CDD standards, as defined in extant KYC Policy, or the OVD has been expired, a Pop-Up message shall be displayed informing the same to the Customer and requesting him to submit one of theOVDs/Tax Proof as per current CDD standards to the Base Branch or carry out Video-KYC.

iv. If no change in customer information, proceed for KYC Updation and select 'no change'. IBS/PNB ONE shall interact with CBS on real-time basis through API for updation in customer account/ID. CBS shall update the KYC updation date in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no through SMS.

v. In case of any change in KYC information/address, customer will be provided following option to update his KYC information/current address either by submitting self-declaration or undertaking online OTP based e- KYC as under:

Option 1: Updation of customer details through IBS/PNB ONE:

a) The customer shall submit the self-declaration with details of current address and annual income/annual turnover (wherever applicable) on IBS/PNB ONE.
b) The Bank is required to verify the declared address through positive confirmation within two months by means such as address verification letter, contact point verification, deliverable, etc.
c) Accordingly, on obtaining the details, a message shall be displayed to the customer informing that a positive confirmation letter with an T-PIN of 6 digits shall be mailed to the current address, declared by the customer, by mail/post, which will be required to be entered at the confirmation page in IBS/PNB ONE for successful updation of KYC.

d) A menu option shall be customized by ITD, wherein the existing address and the declared address shall be captured in CBS from IBS. Both the existing & new address shall be maintained through this menu option. Further, the new declared address and KYC updation date shall also be updated in CRM.
e) An option shall be provided to a designated CASA Back-Office in its admin module for downloading system generated confirmation letters with 6 digit T-PIN for a day/period. The back office user shall download, print and dispatch these confirmation letters, as per Bank guidelines, maintaining all the records on daily basis.
f) Customer on receiving the letter, shall be required to login in his/her IBS/PNB ONE and will be required to enter the 6 digit T-PIN. Upon successful authentication, the IBS/PNB ONE server shall submit the information on real-time basis through API/web services or in batch mode at the end of day, to CBS for further processing.
g) The confirmation process needs to be completed within 60 days

from the updation date in CBS. Upon successful confirmation, the CBS shall update the flag for the positive confirmation.

h) CBS shall update the KYC updation and KYC details in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.
i) For such records, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.
j) However, if customer fails to verify the declared address by T-PIN verification within 60 days, the CBS shall update the same in the newly customized menu option (updating the status as confirmation failed) and the previous address shall again be updated in the CRM and status quo shall be maintained in CBS/CRM.

Option 2*: e-KYC through IBS/PNB ONE:

a) The Customer who is willing to carry out e-KYC, may undergo e-KYC through IBS/PNB ONE module, wherein the Customer shall undertake OTP-based Aadhaar authentication and shall submit self- declaration with details of current address and annual income/annual turnover (wherever applicable).
b) On successful completion of the authentication and obtention of self- declaration of current address of the customer, the IBS/PNB ONE server shall submit the information on real-time basis through API/web services or in batch mode at the end of day, to CBS for further processing.
c) CBS shall update the KYC details and KYC updation date in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.
d) For such records, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.

*Till the time Option 2 is customized, Option 3, hereunder, may be made available for Customer

Option 3: Refer to V-CIP solution:

a) The Customer on selecting 'Option 2', shall be redirected to V-CIP solution, made available on internet, whereupon a separate option for KYC updation is planned to be made available. The customer shall complete the process on V-CIP as detailed at S

No. 4.

b) Accordingly, KYC details and KYC updation date shall be updated in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

vi. For KYC Updation carried out, as detailed above, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.

2. ACCOUNTS OF CUSTOMER, WHO WERE MINOR AT THE TIME OF OPENINGACCOUNT, ON BECOMING MAJOR

In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the base branch. Wherever required, branch may carry out fresh KYC of such customers, i.e., customers for whom account was opened when they were minor, on their becoming a major. As the KYC documents are to be maintained at base branch, the customer may contact his/her base branch or use V-CIP for updation.

3. CHANNELS FOR PERIODIC UPDATION OF CUSTOMERS OTHER THAN INDIVIDUALS

3.1. No change in KYC Information:

In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration (letter from an official authorized by the LE in this regard, board resolution, etc.) in this regard shall be obtained from the LE customer through its email id registered with the Bank/ by post/ by visiting the base branch. Further, branch shall ensure during this process that Beneficial Ownership (BO)/Authorized Signatories information available with them is accurate and shall update the same, if required, to keep it as up to date as possible.

3.2. Change in KYC information.

In case of change in KYC information, the concerned office shall undertake the KYC process equivalent to that applicable for on boarding a

new LE customer.

4. V-CIP FOR PERIODIC UPDATION FOR INDIVIDUAL CUSTOMERS

i. On V-CIP home page, a separate option for KYC Updation shall be made available. Customer shall choose this option and will select the type of KYC updation and Data modification required. For example, Periodic Updation with no change in data, Periodic updation with change in Data, Address Update, Minor to Major, etc.

ii. Customer will accept the conditions and pre-requisites to proceed ahead. Customer will enter his Account Number and the system will fetch the Registered Mobile No. from CBS based on account number and send OTP on that Mobile No. After successful OTP validation, CBS will return customer data from CRM to V-CIP system and customer will move to next page.

iii. Customer will be asked to submit PAN (If already available in system, the same shall be displayed to Customer for verifying the correctness) and Aadhaar (Support for other documents as per RBI guidelines will be subsequently added after Re-KYC flow is implemented). PAN will be directly validated from NSDL and Aadhaar will be verified through OTP base e-KYC process. On successful validation of PAN & Aadhaar, customer will move to next screen.

iv. On first page, customer will be shown his personal details like Name, gender, DOB, Address, etc. The fields will be shown in a format that helps the customer to compare the existing data with Bank and data received from e-KYC.

v. Customer will be given option to update existing data with the data received from e-KYC except Name. The existing data except name can also be overwritten with data received from e-KYC.

vi. Certain other fields can also be allowed to be modified by the customer without providing any documentary evidence such as Father Name (Only if previous entry is blank), Mother Name (Only if previous entry is blank), Marital Status, Spouse Name (Only if marital status selected as married), Annual Income, Expected Annual Credit, etc.

vii. Upon successful completion, KYC details and KYC updation date shall be updated in CRM and an acknowledgement of successful KYC updation shallbe sent to Customer on his/her registered mobile no. through SMS.

viii. However, in case of change of status of customer from minor to becoming an major, the customer shall also be required to undertake complete V-CIP procedure, similar to that of on-boarding of an customer. On successful completion of V-CIP, the V-CIP server shall submit the information on real-

time basis through API/web services or in batch mode at the end of day, to CBS for further processing. CBS shall update the KYC updation and KYC details in CRM and an acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

ix. For aforesaid cases, ITD to customize a mechanism for centralized uploading of KYC records/details at CKYCR.

5. Customer's PAN details, if available with the Bank, is required to be verified from the database of the issuing authority at the time of periodic updation of KYC.

6. In order to ensure customer convenience, updation / periodic updation of KYC can be carried out through e-KYC authentication mode by visiting any branch. Customers who are not willing to undertake e-KYC authentication and express difficulty in approaching the Base branch due to age related or other issues, such customers may approach the Branch Head or Section In charge of Non-Base branch, i.e., any branch, who shall obtain the KYC documents as per Current CDD standards, attest the same, update in CBS and send scanned copy of all the documents to Base branch for record and CKYCR purpose in both the cases.

Annexure- IA

Standard Operating Procedure to Know Your Customer/Subscribers for onboarding for National Pension System in CBS, KYC Updation and Risk Categorization.

A customer can register for NPS (TIER 1+ TIER 2) account or only for TIER 1 account through 'HNPSREG' Menu Option.

Branch officials after verifying NPS registration form and KYC documents, capture data in CBS through menu HNPSREG.

User has to select Account number available in the records and as provided by the customer in the registration form.

Know Your Customer (KYC) Norms

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

a) No Bank shall allow the opening of or keep any anonymous account or account in fictitious names or open account of any person 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).

b) Bank shall verify the identity, address and recent photograph in compliance with provision as specified in PML Rules.

c) At any point of time, where banks 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.

d) Bank may perform KYC process by any of the following methods:

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

   ii) Aadhaar based KYC through offline verification Or

iii) Digital KYC as per PML Rules Or

e) 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 Bank/PoP 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

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

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

h) 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

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

It is imperative to identify and report cases where contribution is disproportionate to income.

Risk Assessment and Risk Categorization

A. While assessing the subscriber's risk profile under pensions schemes regulated / administered by PFRDA, RE may inter-alia take into account the following:

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)
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)

3. Contributions towards NPS Tier I account on a voluntary basis (These accounts generally involve moderate risk)
4. Voluntary contributions towards NPS Tier II account, which is a withdrawable account (These accounts involve generally higher risk in comparison to other categories)

B. Notwithstanding anything contained in A above, while assessing the subscriber's risk profile, RE shall consider the following factors

j) 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
k) Source of contribution
l) Mode of contribution (Cash / Online / Cheque / DD / Card / employers bank account etc)
m) Regularity in the flow of contribution (For eg - Contributions under employer and employee relationship)
n) Withdrawals under Tier I and Tier II account
o) Residence status of subscriber (For eg - Subscribers residing in jurisdiction with higher national risk assessment)
p) Politically Exposed Person
q) Contributions made by the subscriber vis-a-vis the declared income / income range.

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

Banks 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 bank/PoP-SP 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 bank should be commensurate to its size, geographical presence, complexity or activities / structure etc.

The documented risk assessment shall be updated from time to time. The bank 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.

Risk Categorization:

Risk categorization shall be undertaken based on parameters detailed at clause 9.1 and 9.2 of PFRDA Master Circular/2024/04/PoP-02 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).

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 subscriber's profile is to be carried out.

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

1. For opening only Tier-1 account:

At the time of opening NPS Tier-1 account, system will check the existing risk categorization of the customer as well as date of last KYC updation based on the account details provided by the customer and display the same on the screen.

(a) For Low risk customers, risk category will be updated to medium risk and system will check and display pop-up message on the CBS screen regarding KYC status. If KYC updation date is more than 8 years from present date i.e. NPS Tier-1 account opening date, fresh KYC of the customer will be updated in CBS.

If KYC updation date is less than 8 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low risk to medium risk.

(b) For medium and high-risk customers, risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before opening of new NPS Tier-1 account, KYC is to be updated in CBS.

2. For opening both Tier-1 and Tier-2 for new NPS account:

At the time of opening NPS account under category "NPS Tier 1 & Tier-2 both" in CBS, system will check the existing risk categorization of the customer as well as date of last KYC updation based on the account details provided by the customer and display the same on the screen.

(a) For Low/Medium risk customers, risk category will be updated to High Risk NPS and system will check and display pop-up message on the CBS screen regarding KYC status. If KYC updation date is more than 2 years from present date i.e. NPS Tier-2 account opening date, fresh KYC of the customer will be updated in CBS. If KYC updation date is less than 2 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low/medium risk to High Risk.

(b) For existing high-risk customers, risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before opening of new Tier 2 account, KYC is to be updated in CBS.

*In case of Tier II account, where subscriber is Politically Exposed Person (PEP) – Risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before opening of new NPS Tier-1 account, KYC is to be updated in CBS.

Risk assessment for New Business Practices / Developments:

Bank shall pay special attention to money laundering threats that may arise from

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

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

Review of Risk Categorization for Existing Subscribers/customers:

(A) NPS Tier 1 account customers: Risk categorization of all the existing low risk customers having NPS Tier-1 accounts should be changed to medium risk category and system will check and display pop-up message on the CBS screen regarding KYC status.
If KYC updation date is more than 8 years from present date i.e. date of transaction in NPS Tier-1 account, fresh KYC of the customer will be updated in CBS.

If KYC updation date is less than 8 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low risk to medium risk.

For medium and high-risk customers, risk category will remain unchanged. However, system will check updation of KYC as per existing risk category. If KYC updation is due, then before further NPS transaction, KYC is to be updated in CBS.

(B) NPS Tier 2 account customers: Risk categorization of all the existing low/medium risk customers having NPS Tier-2 accounts should be changed High Risk NPS category.

System will check the existing risk categorization of the customer as well as date of last KYC updation based on the account details provided by the customer and display the same on the screen.

If KYC updation date is more than 2 years from present date i.e. transaction in NPS Tier-2 account, fresh KYC of the customer will be updated in CBS. If KYC updation date is less than 2 years, there is no need of any fresh KYC updation. Only risk categorization will be updated from low/medium risk to High Risk.

For existing high risk customers, risk category will remain unchanged. However system will check updation of KYC as per existing risk category. If KYC updation is due, then before NPS transaction, KYC is to be updated in CBS.

In case of KYC due, Pop-up message to be displayed at CBS during NPS transaction done by the customer through branch and an SMS should be also sent to customer for updation of fresh KYC as per existing process of KYC updation.

Review of Risk Categorization for Existing Subscribers/customers at the time of Exit from NPS:

At the time of exit from National Pension System due to superannuation, death of subscriber or premature exit, KYC status of the customer will be updated as per the existing KYC policy of the Bank.

Presently request of customer for exit from NPS is processed as mentioned below:

(a) Offline – Duly verified physical forms from the branches sent to Government Business Department, General Banking Division, HO for processing the same in the CRA portal.
(b) Online - Request for exit from NPS (superannuation & premature exit) is submitted by the customer through subscriber login on the CRA portal. Further the request is verified in the CRA portal by dealing officials at Government Business Department, General Banking Division, HO.

A new module in CBS is to be customized for marking exit of a customer from NPS (offline mode – to be developed by Government Business Department, General Banking Division, HO) after processing of exit request on the CRA portal. Subsequently system will update the KYC status for the customer/subscribers in CBS accordingly.

Annexure-II

Digital KYC Process

A. An application for digital KYC process to be developed by the bank which shall be made available at customer touch points for undertaking KYC of its customers and the KYC process shall be undertaken only through this authenticated application of the Bank.
B. The access of the Application shall be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Bank to its authorized officials.
C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.
D. It is to be ensured that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Bank shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photographof the customer.
E. The Application of the Bank shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For

example, in case of physical Aadhaar/ eAadhaar downloaded from UIDAI where QR code isavailable, the details like name, gender, date of birth and address can be auto- populated by scanning the QR available on Aadhaar/ e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Bank shall not be used for customer signature. The Bank must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Bank. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Bank, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the Bank shall check and verify that:-
   a information available in the picture of document is matching with the information entered by authorized officer in CAF.
   b live photograph of the customer matches with the photo available in thedocument.; and
   c all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the Bank who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Bank may use the services of Business Correspondent (BC) for this process.

Annexure – III

INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS, I.E., CUSTOMER BEHAVIOUR AND RISK BASED TRANSACTION MONITORING, HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/ LOCATIONS/ALERTS FOR BRANCHES/ OFFICES

1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

i. Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
ii. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
iii. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
iv. Customer giving confusing details about a transaction.
v. Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.
vi. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
vii. Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
viii. Customer's representatives avoiding contact with the branch.
ix. Customers who repay the problem loans unexpectedly.
x. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
xi. Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
xii. Customer regularly issues large value cheques without balance and then deposits cash.
xiii. Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions Involving Large Amounts of Cash

i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
iii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
iv. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
v. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
vi. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange, etc.;
vii. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

B. Transactions that do not make Economic Sense

i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
ii. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

C. Activities not consistent with the Customer's Business

i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
ii. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.
iii. Unusual applications for DD/TT/PO against cash.
iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.

v. Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid Reporting/Record-keeping Requirements

i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
iii. An account where there are several cash deposits/withdrawals below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities

i. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.
ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
iii. Funds coming from the list of countries/centers, which are known for money laundering.

F. Customer who provides Insufficient or Suspicious Information

i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
ii. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
iii. A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain Suspicious Funds Transfer Activities

i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.

iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. Certain Bank Employees arousing Suspicion

i. An employee whose lavish lifestyle cannot be supported by his or her salary.
ii. Negligence of employees/willful blindness is reported repeatedly.

I. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

J. Some examples of suspicious activities/transactions to be monitored by the operating staff-

i. Large Cash Transactions
ii. Multiple accounts under the same name
iii. Frequently converting large amounts of currency from small to large denomination notes
iv. Placing funds in term Deposits and using them as security for more loans.
v. Large deposits immediately followed by wire transfers.
vi. Sudden surge in activity level.
vii. Same funds being moved repeatedly among several accounts.
viii. Multiple deposits of money orders, Banker's cheques, drafts of third Parties
ix. Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
x. Cheques of third parties into the account followed by immediate cash withdrawals.
xi. Transactions inconsistent with the purpose of the account.
xii. Maintaining a low or overdrawn balance with high activity.

Check list for preventing money-laundering activities:

i. A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).

ii. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
iii. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
iv. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
v. A customer experiences increased wire activity when previously there has been no regular wire activity.
vi. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
vii. A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
viii. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
ix. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
x. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
xi. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.
xii. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
xiii. Periodic wire transfers from a person's account/s to Bank haven countries.
xiv. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
xv. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques.
xvi. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when the amount is very large (say over Rs.10 lakhs), the amount is just under

a specified threshold, the funds come from a foreign country or such transactions occur repeatedly.

xvii. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold).

xviii. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

2. INDICATIVE LIST OF HIGH RISK CUSTOMERS

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban*

ii. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities*

iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations

iv. Customers with dubious reputation as per public information locally available or commercially available.

v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk

vi. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations, etc.

vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.

viii. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner (UBO);

ix. Non-resident customers and foreign nationals

x. Accounts of Embassies / Consulates;

xi. Off-shore (foreign) corporation/business

xii. Non face-to-face customers

xiii. High net worth individuals [HNIs]

xiv. Firms with 'sleeping partners'

xv. Companies having close family shareholding or beneficial ownership

xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
xvii. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence
xviii. Investment Management / Money Management Company/Personal Investment Company
xix. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
xx. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
xxi. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations (UN) or its agencies)
xxii. Money Service Business: including seller of: Money Orders / Travelers‟ Checks / Money Transmission /Check Cashing / Currency Dealing or Exchange
xxiii. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
xxiv. Gambling/gaming including "Junket Operators" arranging gambling tours
xxv. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
xxvi. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries).
xxvii. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
xxviii. Customers that may appear to be Multi-level marketing companies, etc.

*No fresh account to be opened if name appears in the list. However, if any existing account is placed in the list subsequently, the same shall be freezed and placed in high risk till its final closure.

3. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

i. Non-Bank Financial Institution
ii. Stock brokerage
iii. Import / Export
iv. Gas Station
v. Car / Boat / Plane Dealership
vi. Electronics (wholesale)
vii. Travel agency
viii. Used car sales
ix. Telemarketers
x. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
xi. Dot-com company or internet business
xii. Pawnshops
xiii. Auctioneers
xiv. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
xv. Sole Practitioners or Law Firms (small, little known)
xvi. Notaries (small, little known)
xvii. Secretarial Firms (small, little known)
xviii. Accountants (small, little known firms)
xix. Venture capital companies

4. LIST OF HIGH / MEDIUM RISK PRODUCTS & SERVICES

i. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), etc.
ii. Electronic banking
iii. Private banking (domestic and international)
iv. Trust and asset management services
v. Monetary instruments such as Travelers' Cheque
vi. Foreign correspondent accounts
vii. Trade finance (such as letters of credit)
viii. Special use or concentration accounts
ix. Lending activities, particularly loans secured by cash collateral and marketable securities
x. Non-deposit account services such as Non-deposit investment products and Insurance
xi. Transactions undertaken for non-account holders (occasional customers)

xii. Provision of safe custody and safety deposit boxes
xiii. Currency exchange transactions
xiv. Project financing of sensitive industries in high-risk jurisdictions
xv. Trade finance services and transactions involving high-risk jurisdictions
xvi. Services offering anonymity or involving third parties
xvii. Services involving banknote and precious metal trading and delivery
xviii. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES

Countries/Jurisdictions

i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR").
ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.
vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
vii. Countries identified by credible sources as having significant levels of criminal activity.
viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations

i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.

iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

5. INDICATIVE LIST OF HIGH RISK COUNTRIES:

The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

Annexure-IV

KYC documents for eligible FPIs under PIS

		FPI Type		
Document Type		**Category I**	**Category II**	**Category III**
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation, etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution @@	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors / Partners / Trustees, etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Authorized Signatories	List Signatures and	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare "no UBO over25%")	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators / Law Enforcement Agencies the relative document/s would be submitted to the bank.				
@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose ofopening bank accounts, etc., is not in vogue, may submit 'Power of Attorney granted to Global Custodian / Local Custodian in lieu of Board Resolution'				

Category	Eligible Foreign Investors
I.	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International / Multilateral Organizations / Agencies.
II.	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance / Reinsurance Companies, Other Broad Based Funds, etc. b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers, etc. c) Broad based funds whose investment manager is appropriately regulated. d) University Funds and Pension Funds. e) University related Endowments already registered with SEBI as FII/ Sub Account.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies / Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Annexure-V

FREQUENTLY ASKED QUESTIONS (FAQs)

Q 1. What is KYC?

Response: KYC is an acronym for "Know your Customer" a term used for Customer identification process. It is a process by which banks obtain information about the identity and address of the customers while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity.

It involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, financial status & nature of customer's business, reasonableness of operations in the account in relation to the customer's overall profile, etc., which in turn helps the banks to manage their risks prudently.

Q 2. What is the objective of KYC?

Response: The objective of the KYC guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities.

KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently and enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank's Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

Q 3. What is Money Laundering and Terrorist financing?

Response: Money laundering refers to conversion of money illegally obtained to make it appear as if it originated from a legitimate source. Money laundering is being employed by launderers worldwide to conceal criminal activity associated with it such as drugs /arms trafficking, terrorism and extortion. Terrorist financing means financial support to, in any form of terrorism or to those who encourage, plan or engage in terrorism. Money launderers send illicit funds through legal channels in order to conceal their criminal origin while those who finance terrorism transfer funds that may be legal or illicit in original in such a way as to conceal their source and ultimate use, which is to support Terrorist financing.

Money laundering has become a pertinent problem worldwide threatening the stability of various regions by actively supporting and strengthening terrorist networks and criminal organizations. The links between money laundering,

organized crime, drug trafficking and terrorism pose a risk to financial institutions globally. Government of India has promulgated Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and RBI Master Direction on KYC, enforces legal/statutory/regulatory obligations on both bank and customers to provide KYC information/documents.

Q 4. Whether KYC is mandatory?

Response: Yes. It's a regulatory and legal requirement.

i. Regulatory: - In terms of the guidelines issued by the Reserve Bank of India (RBI) on 29 November, 2004 on Know Your Customer (KYC) Standards - Anti Money Laundering (AML) measures, all banks are required to put in place a comprehensive policy framework covering KYC Standards and AML Measures.

ii. Legal:- The Prevention of Money Laundering Act, 2002 (PMLA) which came into force from 1st July, 2005 (after "rules" under the Act were formulated and published in the Official Gazette) also requires Banks, Financial Institutions and Intermediaries to ensure that they follow certain minimum standard of KYC and AML as laid down in the ACT and the "rules" framed thereunder.

Q 5. Is KYC information obtained from customer kept confidential?

Response: Yes, the customer profile/information collected by the Bank at the time,of account opening or otherwise, are kept confidential and are not disclosed to any person, except when required under the provisions of applicable laws and regulations or where there is a duty to the public to disclose or the interest of bank requires disclosure.

Q 6. What are the documents to be obtained from customers as 'proof ofidentity' and 'proof of address'?

Response: The Government of India has notified six documents or its equivalent e- documents as 'Officially Valid Documents (OVDs) for the purpose of producing proof of identity of individual customers. These six documents are the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

You need to submit any one of these documents as proof of identity. If these documents also contain your current address details, then it would be accepted

as 'proof of address'. Provided that if customer is desirous of receiving any benefit or subsidy under any scheme notified under Aadhaar Act, 2016, customer shall be required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

KYC documents to be obtained from non-individual customers have been specifiedin the KYC policy.

Q 7. If customer do not have any of the OVDs listed above with current updated address, can customer provide other OVD?

Response: Yes, customer can provide the following documents or the equivalent e- documents for the limited purpose of proof of address, with an undertaking along with AOF/OVDs stating that he/she shall submit his OVD with updated current address within 3 months failing which operations in his/her account shall be restricted.

i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. Property or Municipal tax receipt;
iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

However, if customer undertakes Aadhaar authentication using e-KYC facility of UIDAI and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository (CIDR), he may give a self-declaration to that effect.

Q 8. Are there any additional documents to be obtained from customer apart from 'proof of identity' and 'proof of address'?

Response: Yes, atleast one document or the equivalent e-document thereof in support of **nature of business** and **financial status of the customer** such as:-

i. Salary slip/Form-16,
ii. Registration certificate,
iii. CST or VAT or GST certificates,
iv. Income tax returns or Sales tax or GST returns,
v. Licence / certificate of practice issued by any professional body

incorporated under a statute,

vi. Certificate / licence issued by the municipal authorities under Shop and Establishment Act,
vii. Further, in respect of customers who don't have any business / financial activity or don't have any such proof such as housewife, student, minor, labour working in un-organized sector, farmers, etc., may submit self-declaration to this effect.
viii. Similarly, in case of Customers drawing pension from our Branches and maintaining Pension/Term Deposit Accounts, the Branches may self-assess their income from Bank Account Statement/Interest Certificate, as the case maybe, and obtain self-declaration/documents in support of other income, if required, from such Customers.
ix. Since the above list of documents is only indicative, the branch may obtain any other document in support of nature of business and financial status of the customer, as they deem fit.

Q 9. What if the customer doesn't have any document in support of nature of business, financial status, annual income?

Response: Customers who don't have any business / financial activity or don't have any such proof such as housewife, student, minor, labour working in un-organized sector, farmers, etc., may submit self-declaration to this effect.

Q 10. If customer does not have any of the documents listed above to showhis/her 'proof of identity', can he/she still open a bank account?

Response: Yes, customer can still open a bank account known as 'Small Account', which entails certain limitations, by submitting his/her recent photograph and putting signature or thumb impression in the presence of a bank official.

Q 11. Is there any difference between such 'small accounts' and other accounts?

Response: Yes. The 'Small Accounts' have certain limitations such as:

i. balance in such accounts at any point of time should not exceed ₹50,000
ii. total credits in one financial year should not exceed ₹1,00,000
iii. total withdrawal and transfers should not exceed ₹10,000 in a month.
iv. Foreign remittances cannot be credited to such accounts.

Such accounts remain operational initially for a period of twelve months and thereafter, for a further period of twelve months, if the holder of such an account provides evidence to the bank of having applied for any of the officially valid documents within twelve months of the opening of such account. The bank will review such account after twenty four months to see if it requires such

relaxation.

Q 12. If customer refuses to provide requested documents for KYC to the bankfor opening an account, what may be the result?
Response: If customer does not provide the required documents for KYC, the bank shall not open the account.

Q 13. Can a customer open bank account with only an Aadhaar card?
Response: As per RBI directions, Aadhaar card is now accepted as a proof of both,identity and address. However, PAN/Form 60 along with one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status is also required.

Q 14. Is Aadhaar mandatory for opening of an account?
Response: No, Aadhaar is not mandatory for opening of an account. As per RBI directions, only an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016) is mandatorily required to provide Aadhaar and is required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

Q 15. What is e-KYC? How does e-KYC work?
Response: e-KYC refers to electronic KYC. e-KYC is possible only for those who have Aadhaar number or proof of possession of Aadhaar. While using e-KYC service, customer has to authorise the Unique Identification Authority of India (UIDAI), by explicit consent, to release his/her identity/address through biometric authenticationto the bank branches/business correspondent (BC). The UIDAI then transfers his/her data comprising name, age, gender, and photograph of the individual, electronically to the bank/BC. Information thus provided through e-KYC process is permitted to be treated as an 'Officially Valid Document' under PML Rules and is a valid process for KYC verification.

Q 16. Is introduction necessary while opening a bank account?Response:
Response: No, introduction is not required.
Q 17. Can a customer transfer his existing bank account from one branch to another?
Response: KYC verification once done by one branch / office of the Bank shall be valid for transfer of the account to any other branch / office of the same Bank, providedfull KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Q 18. Is a customer required to furnish KYC documents for each account

he/she opens in the Bank?

Response: As per RBI guidelines, an individual customer can maintain only a single Unique Customer ID Code (UCIC)/Customer-ID in a Bank and all the accounts of the customer have to be opened/ linked under this Customer-ID. Therefore, if a customer has opened an account with the Bank, which is KYC compliant, then for opening another account, furnishing of documents is not necessary.

Q 19. Customer's KYC was completed when he/she opened the account. Why does Bank ask for doing KYC again?

Response: In terms of RBI guidelines, Bank is required to periodically update KYC records. This is a part of ongoing due diligence on bank accounts. The periodicity of such updation varies from account to account or categories of accounts depending on the Bank's perception of risk. Further, the Bank may insist for KYC updation, whenever there is a doubt about the authenticity or adequacy of the customer identification data (CID) it has obtained.

Q 20. Do the customer need to submit KYC documents to the bank while purchasing third party products (like insurance or mutual fund products) from banks?

Response: Yes, all customers who do not have accounts with the Bank (known as walk-in customers) have to produce proof of identity and address while purchasing third party products from Bank if the transaction is for ₹50,000 and above. KYC exercise may not be necessary for bank's own customers for purchasing third party products. However, instructions to make payment by debit to customers' accounts or against cheques for remittance of funds/issue of travellers' cheques, sale of gold/silver/platinum and the requirement of quoting PAN number for transactions of ₹50,000 and above would be applicable to purchase of third party products from Bank by Bank's customers as also to walk-in customers.

Q 21. What does obtaining a certified copy by the Bank mean?

Response: Obtaining a certified copy by bank shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Branch under his GBPA/PF no. Branch Official will also attest the duly signed photograph of the customer.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin
(PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by

any one of the following, may be obtained:

i. authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
ii. branches of overseas banks with whom Indian banks have relationships,
iii. Notary Public abroad,
iv. Court Magistrate,
v. Judge,
vi. Indian Embassy/Consulate General in the country where the non-residentcustomer resides.

Q 22. What documents are required for opening an account of partnership(registered) firm?

Response: For opening an account of a partnership (registered) firm, the certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

i. Registration certificate;
ii. Partnership deed;
iii. Permanent Account Number of the partnership firm;
iv. Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
v. the names of all the partners and
vi. address of the registered office, and the principal place of its business, if it is different.

Q 23. What documents are required for opening an account of trust (registered)?

Response: For opening an account of a trust (registered), certified copies of eachof the following documents or the equivalent e-document thereof shall be obtained:

i. Registration certificate;
ii. Trust deed;
iii. Permanent Account Number or Form No.60 of the trust;
iv. Documents, as specified in Section 2, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
v. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
vi. the address of the registered office of the trust; and
vii. list of trustees and documents, as are required for individuals under Section 2 for those discharging role as trustee and authorised to

transact on behalf of the trust.

Q 24. What do you mean by equivalent e document?

Response: 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 customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. Further, at present, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.

Q 25. Does our bank has facility to open accounts of an individual customer using OTP based e-KYC, in non face to face mode?

Response: Yes, our bank has implemented facility to open accounts of an individual customer using OTP based e-KYC, in non face to face mode. For details staff may refer guidelines issued vide Operations Division (CASA Back Office) Circular No. 6/2021 & Operations Division (Back Office Section) Circular No. 09/2021.

Q 26. Does our bank has facility to open accounts of an individual customer using Video based Customer Identification Process?

Response: Yes, our bank has implemented facility to open accounts of an individual customer using Video based Customer Identification Process. For details staff may refer guidelines issued vide Operations Division (CASA Back Office) Circular No. 6/2021 & Operations Division (Back Office Section) Circular No. 09/2021.

Q 27. What is the meaning of proof of possession of AADHAAR number?

Response: The Aadhaar number holder can use any of the following documents to prove possession of Aadhaar number subject to the concerned entity's right to verifythe genuineness of the below mentioned documents. For details 'The Unique Identification Authority of India Notification No. 13012/184/2019/Legal/UIDAI (No. 2 of 2019) dated 04th April 2019' may please be referred.

(a) Aadhaar letter: Issued by the Authority carries name, address, gender, photo and date of birth details of the Aadhaar number holder.

(b) Downloaded Aadhaar (e-Aadhaar): Carries name, address, gender, photo and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by the Authority as per

Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

(c) Aadhaar Secure QR Code: A quick response code generated by the Authority containing name, address, gender, photo and date of birth details of the Aadhaar number holder. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

(d) Aadhaar Paperless Offline e-KYC: An XML document generated by the Authority containing name, address, gender, photo and date of birth details of the Aadhaar number holder. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

Q 28. Is there any Standard Operating Procedure in our Bank for exception handling during e-KYC?

Response: In case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, it shall be ensured that apart from obtaining the Aadhaar number, identification to be performed preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 2.4.2 (c) of policy document. It is to be ensured to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review. The detailed operational guidelines and SOP have been circulated vide PSFID / Financial Inclusion / Circular No. 06 / 2019 dated 26.09.2019.

Q 29. Can the name of a customer be modified on the basis of updation done in OVD & PAN?

Response: Yes, the name of a customer can be modified on the basis of updation done in OVD & PAN, subject to Bank's right to verify the genuineness of the documents.

Q 30. How can a Special Rupee Vostro Account(SRVA) of a Non-Resident Bank not having PAN number be opened in CBS?

Response: Opening of Special Rupee Vostro Account (SRVA) of Non-Resident Bank may not require PAN in the Bank's CBS. Unique Code allotted by RBI will mandatorily be validated and captured in CBS.

Q 31. What KYC documents are required to open account of a Nepali Citizen?

Response: Extant KYC Policy of Bank which is in line with RBI Master Direction on KYC provides no distinction between CDD procedure to be followed for type of Individuals; Indians and Foreign Nationals.

As regards opening an account where an individual does not possess an OVD, RBI guidelines permit opening a "Small Account" as specified in extant KYC Policy of Bank.

Further where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Glossary

Abbreviation	Description
AI	Artificial Intelligence
AML	Anti-Money laundering
API	Application Programming Interface
ASPs	Annuity Service Providers
BC	Business Correspondents
BF	Business Facilitator
BOs	Beneficial Owner
CAF	Customer Application Form
CAP	Customer Acceptance policy
CBDT	Central Board of Direct Taxes
CBIC	Central Board of Indirect Taxes and Customs
CBS	Core Banking solution
CBWTR	Cross Border Wire Transfer Report
CCR	Counterfeit Currency report
CDD	Customer Due Diligence
CDF	Currency Declaration Form
CEO	Chief executive Officer
CERSAI	Central Registry Of Securitization Asset Reconstruction And Security Interest Of India
CFT	Combating Financing of Terrorism
CIDR	Central Identities Data Repository
CID	Customer Identification Data
CIP	Customer Identification Procedure
CKYCR	Central KYC Records Registry
CPV	Contact Point Verification
CRA	Central recordkeeping Agency
CRS	Common Reporting Standards
CST	Central Sales Tax
CTCR Division	Counter Terrorism and Counter Radicalization Division
CTR	Cash Transaction Report
DGFT	Director General of Foreign Trade
DPMS	Dealers in Precious Metals and Stones
DNFBPs	Designated Non Financial Businesses and Professions
ECS	Electronic Clearing Service
EDD	Enhanced Due Diligence
E-KYC	Electronic – Know Your Customer
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FEDAI	Foreign Exchange Dealer's Association of India

FEMA	Foreign Exchange Management Act
FIU-India	Financial Intelligence Unit- India
FPIs	Foreign Portfolio Investors
FRMD	Fraud Risk Management Division
GPS	Global Positioning System
GST	Goods and Service Tax
HNIs	High Net worth Individuals
HUF	Hindu Undivided Family
IBA	Indian Banks Association
ICSI	Institute of Company Secretaries of India
IEC	Importer Exporter Code
IGA	Inter Government Agreement
IMPS	Immediate Payment System
IRDA	Insurance Regulatory and Development Authority of India
KYC	Know Your Customer
LE	Legal Entity
MAAT	Mutual Administrative Assistance in Tax Matters
MD	Managing Director
MEA	Ministry of External Affairs
MHA	Ministry of Home Affairs
ML	Money Laundering
MLM	Multi Level Marketing
NEFT	National Electronics Funds Transfer System
NGO	Non- Govermental Organization
NPO	Non Profit Organisation
NPS	National Pension System
NREGA	National Rural Employment Guarantee Act
NRI	Non- Resident Indian
NRO	Non- Resident Ordinary
NSDL	National Securities Depository Limited
NTR	Non Profit Organisation Transaction Report
ORMC	Operational Risk Management Committee
OTP	One Time Pin/ Password
OVD	Officially Valid Document
PAN	Permanent Account Number
PEP	Politically Exposed Person
PIO	Person Of Indian Origin
PIS	Portfolio Investment Scheme
PMLA	Prevention of Money Laundering Act
PO	Principle Officer
PoA	Power of Attorney

PoP	Point of Presence
PoP-SP	Point of Presence –Service Provider
PPI	Prepaid Payment Instrument
PPO	Pension Payment Orders
PRAN	Permanent Retirement Account Number
QR Code	Quick Response Code
RBI	Reserve Bank of India
RBTM	Risk- Based Transaction Monitoring
ROC	Registrar of Companies
RTGS	Real Time Gross Settlement
SEBI	Securities and Exchange Board of India
SHG	Self Help Group
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
V-CIP	Video Based Customer Identification Process
VAT	Value Added Tax
UAPA	Unlawful Activities (Prevention) Act
UBO	Ultimate Beneficial Owner
UCIC	Unique Customer Identification Code
UIDAI	Unique Identification Authority of India
UN	United Nations
UNSCRs	United Nation's Security Council resolutions
USA	United States of America
XML	Extensible Mark Up Language