

(Part II-Operational Guidelines)

Operational Guidelines for Know Your Customer (KYC) Policy

Division : Data Privacy & Management Division
Version : 2026_KYC_1.0



ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਈਵੇਸੀ ਏਵ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

Guidelines Custodian

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

Guidelines Version Control

S.N.	Version Number	Version Date	Summary of Changes
1	2023_KYC_1.2	01 Nov 2023	Policy updated as per RBI, Master Directions dated 17.10.2023
2	2024_KYC_1.0	27 Feb 2024	Enhanced Due Diligence – Accounts of Politically exposed persons, Periodic Updation
3	2024_KYC_1.1	10 Dec 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.
4	2025_KYC_1.0	19 Mar 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.
5	2025_KYC_1.1	07 Aug 2025	RBI updated its Master Direction – Know Your Customer Direction, 2016 on 12.06.2025.
6	2025_KYC_1.2	02 Dec 2025	RBI updated its Master Direction – Know Your Customer Direction, 2016 on 14.08.2025.
7	2026_KYC_1.0		Reserve Bank of India (Commercial Banks – Know Your Customer) Directions, 2025 (Updated as on December 29, 2025) and PFRDA updated its Master Direction on 02.12.2025.

Guidelines Governance

Frequency Of Review	Annual
Last reviewed on	04.10.2025
Approval Path	ACE
Supersedes	Data Privacy & Management Division Circular No. 50/2025 dated 02.12.2025

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 Reserve Bank of India (Commercial Banks – Know Your Customer) Directions, unless the context otherwise requires, the 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 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.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs)¹, 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.

[1]. The Person of Indian Origin (PIO) card scheme was withdrawn and merged with the Overseas Citizen of India (OCI) card scheme via Gazette Notification No. 25024/9/2014-F.I on 09.01.2015. Hence "PIO" may be treated as "OCI".

- 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-frozen).
- 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.

Guidelines for NRI and OCI customers under NPS

Admissible digital copy of Officially Valid Document (OVD) for Non Resident Indian (NRI) and Overseas Citizen of India REs, at the time of onboarding the subscriber into NPS, shall identify their subscriber, verify their identity and obtain information for the purpose Customer Due Diligence (CDD). The name as mentioned in the application/KYC form shall match the name as mentioned in the Proof of Identity (PoI) submitted by subscriber. The following documents shall be admissible as Proof of Identity (PoI) and Proof of Address (PoA) for opening of NPS tier I accounts.

For Non-Resident Indian (NRI):

a) The following documents shall be accepted as PoI:

- i. The passport;

b) The following documents shall be accepted as PoA:

- iv. The passport;
- v. Address proof duly certified by the foreign government or foreign public authorities:

- Residence Permit; or
 - Work Permit; or
 - Foreign National ID; or
 - Overseas driver's licence (if government-issued)
- vi. Any other document as notified by the Central Government in consultation with the Regulator

Note:

- i. Where the passport of an NRI subscriber contains both the permanent and current address as foreign addresses, the same shall be accepted as valid Proof of Address (PoA). In such cases, no separate Indian address proof shall be required for Indian correspondence address. The passport copy shall be self-attested by the subscriber and attested by a competent authority (Indian Embassy / Consulate General in the country where the non-resident customer resides / Notary Public / /Court Magistrate/Judge/authorised officials of overseas branches of Scheduled Commercial Banks registered in India).
- ii. Where the Passport of an NRI subscriber contains both the permanent and current address as Indian, the same shall be accepted as valid Proof of Address for Indian address only. However, since the subscriber is residing outside India, a separate document evidencing the current overseas address shall be obtained.
- iii. In case the officially valid document 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.

All such documents shall be self-attested by the subscriber and attested by an authorised official (Indian Embassy / Consulate General in the country where the non-resident customer resides / Notary Public / /Court Magistrate/Judge/authorised officials of overseas branches of Scheduled Commercial Banks registered in India).

For Overseas Citizen of India (OCI):

- a) The following documents shall be accepted as Pol:
- i. The OCI Card; and
 - ii. The foreign passport
- b) The following documents shall be accepted as PoA only if it contains current overseas address:
- i. The foreign passport; or
 - ii. The driving licence (issued by foreign authorities)
- 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 Reserve Bank of India (Commercial Banks – Know Your Customer) Directions/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
- b) the proof of possession of Aadhaar number where offline verification can be carried out; or
- c) 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
- d) the KYC Identifier with an explicit consent to download records from CKYCR; and
- e) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, and
- f) one recent photograph; and
- g) 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 (b) 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 issued 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, including Aadhaar Face Authentication can be done by bank official/business correspondents/business facilitators.

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.

Explanation 4: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer 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), the customer shall provide the Aadhaar number to the bank. In other cases, customers may provide the Aadhaar number voluntarily.

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. The liveness check shall not result in exclusion of person with special needs. For the purpose of 'liveness' check, Bank may use various parameters which not only involves checking the movement of eyelid and eyeball or blinking, but also may use other factors viz live facial expressions, nodding of head, subscriber showing OTP while being clearly visible on-screen, real-time video recording and displaying copies of documents on the screen etc. Where a customer is unable to perform OTP-based or expression-based checks.

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, 2020, and 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 and Establishment 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 office of 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 that 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 following documents 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 thereof 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 along with 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 beneficial owner(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 bank's knowledge about the customers segmentation and risk profile through digital/manual transaction(s) pattern in their accounts/EOD balance, physical visit (if needed) and the justification related to source of funds/wealth up to the satisfaction of bank official in case of any suspicion.

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. RE shall consider the following factors, while doing ongoing due diligence:

- 1) Source of contribution
- 2) Mode of contribution (Cash / Online / Cheque / DD / Card / employers bank account etc.)
- 3) Regularity in the flow of contribution (For eg - Contributions under employer and employee relationship)
- 4) Withdrawals under Tier I and Tier II account under All Citizen Model/Corporate Model or any other scheme as may be approved by PFRDA from time to time.
- 5) Residence status of subscriber (For eg - Subscribers residing in jurisdiction with higher national risk assessment)
- 6) Contributions made by the subscriber vis-a-vis the declared income / income range.
- 7) Verification at the time of exit (superannuation /premature exit / death etc.):
 - i. No payments should be made to third parties on attainment of superannuation except payments to nominee(s)/ legal heir(s) in case of death.
 - ii. Necessary due diligence of the subscriber(s) / nominee(s) / legal heir(s) should be carried out before making the pay-outs/settling claims
- 8) 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. **Any pendency**

resulting from this activity shall be considered a pendency for the subsequent quarter in which the activity is conducted.

- (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).
For NPS subscribers, this is permitted only in case of periodic updation of KYC and not at the time of exit or withdrawal from the All-Citizen /Corporate Model.
- i. **With respect to the periodic updation or re-KYC of NPS subscriber, if there is a change only in address details of the subscriber, the Bank shall preferably obtain a CKYC identifier for updating the address and in case if the same is not available or updated, the bank may obtain a valid OVD depicting the changed address within the timelines as prescribed in the PML rules.**

- ii. In respect of NPS accounts categorized as medium risk, the bank shall allow all transactions and ensure the updation of KYC within six months of its falling due for re-KYC. The bank shall subject accounts of such subscribers to regular monitoring. This shall also be applicable to medium risk accounts for whom periodic updation of KYC has already fallen due. Failure to complete the KYC process within the prescribed timelines shall result in freezing of service requests related to change in investment pattern or pension funds, as well as freezing of partial withdrawal and exit facilities.
- iii. With respect to all high-risk accounts, failure to complete the KYC process within the prescribed timelines shall result in immediate freezing of service requests related to change in investment pattern or pension funds, as well as freezing of partial withdrawal and exit facilities.
- iv. Bank shall ensure that the fields provided by the CRA for recording Risk Category (Low / Medium / High) are duly updated for each account. Bank shall also carry out periodic KYC updation and ensure that the risk categorization of each account is appropriately flagged in the system.
- v. NPS subscriber, shifting from the Government to Private sector, a fresh KYC needs to be undertaken through any of the modes permitted under these guidelines.
- vi. NPS subscriber, shifting from one RE to another RE, the latter may perform the KYC preferably by using CKYC identifier, in case the same is not available, the KYC process may also be performed by other modes as mentioned in these guidelines.
- vii. In case of NRI/OCI subscribers, the updation/ periodic updation of KYC records are allowed to be carried out at any overseas branch of the RE with which subscriber maintains the NPS account.
- viii. The updation/periodic updation of KYC records are allowed to be carried out at any overseas branch of the RE with which subscriber maintains the NPS account.
- ix. In case of existing NRI/OCI subscribers, the requirement of physical location of subscriber being in India shall be relaxed for re-KYC / KYC modification for existing subscribers.
- x. During periodic updation, the subscriber shall reconfirm FATCA/CRS declarations, tax residency details, and current residency status (NRI/OCI/Resident) to ensure compliance with applicable FEMA and PMLA provisions.
- 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).

iii. 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 Policy *ibid*. It is, however, reiterated that the ultimate responsibility for periodic updation of KYC remains with the bank concerned.

iv. **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.

v. 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.

vi. 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.

vii. 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 **updatation / periodic updatation**. Further, it shall be ensured that the information/ documents obtained from the customers at the time of **updatation / periodic updatation** 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 (in upcoming quarters), it is to be ensured to give the client three notices 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. The bank shall expeditiously implement the same but not later than January 01, 2026.

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^[2]. 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.

[2]. The Person of Indian Origin (PIO) card scheme was withdrawn and merged with the Overseas Citizen of India (OCI) card scheme via Gazette Notification No. 25024/9/2014-F.I on 09.01.2015. Hence "PIO" may be treated as "OCI".

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.

24. Additional guidelines for NRI and OCI customers under NPS

In case the RE suspects that the documents furnished for establishing NRI/OCI status are forged, tampered, or otherwise unreliable, the RE shall classify the subscriber as highrisk, undertake enhanced due diligence, reject the KYC application, and file a Suspicious Transaction Report (STR) with FIU-IND in accordance with Rule 9 of the PML Rules and other applicable regulatory guidelines.

B. Simplified Due Diligence

25. 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.

26. 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.

27. 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.

28. 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, including the 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.

- 28A.** 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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 SENSRT — 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 there is 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-III** 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) Chartered 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;

33A 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.

34. 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.
- (vi) 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

35. 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

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

- (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://www.un.org/securitycouncil/sanctions/1988/materials>.

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.

36. 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-I of Reserve Bank of India (Commercial Banks – Know Your Customer) Directions as amended from time to time**).

36A 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-I of Reserve Bank of India (Commercial Banks – Know Your Customer) Directions 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.

37. 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 II of Reserve Bank of India (Commercial Banks – Know Your Customer) Directions 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.

38. 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.

38A. 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.

38B. 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.

39. 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.

39A. Banks are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanction requirements.

Other Instructions

40. 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 the customer.
- 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

40A. 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

41. 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 on customer's consent, 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.

[Explanation: The RE that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, any bank downloading and relying on such records from the CKYCR shall not be required to re-verify the authenticity of the customer's identity and / or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. The bank downloading and relying on KYC records downloaded from the CKYCR shall remain responsible for all aspects of CDD procedure and provisions of these Directions, except verification of identity and / or address 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.**

- I. 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 (PML 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.

C) In case of every new subscriber including persons with disabilities, necessary client due diligence with valid KYC of the subscriber shall be done at the time of commencement of account-based relationship, such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high-risk subscribers. Bank shall avoid collection of KYC documents repeatedly from subscribers including persons with disabilities during subscriber for onboarding and to use the CKYCR unique number as the primary reference for establishing an account-based relationship. Further, Bank shall ensure the reporting requirements under the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) as amended by RBI from time to time. Accordingly, Bank shall develop and implement a mechanism where subscribers who have already completed their KYC process with one regulated entity may authorize the sharing of their KYC information with other entities through the Central KYC Registry (CKYC).

Further, with respect to person with disabilities, the following may be referred:

(D) Establishing an account-based relationship can be performed in the name of persons with disabilities.

(E) Every person who has attained the age of eighteen years is considered as major. Only a major, who is of sound mind and is not disqualified from contracting by law is competent to enter into contract. In accordance with the provisions of the Mental Health Care Act, 2017 and the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999, if the individual would require a guardian, the intermediary may rely upon the Guardianship Certificate issued by the Local Level Committee under the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999.

(F) If a person with disability is unable to sign for himself / herself, the account can be opened with his/her thumb impression or with the signature of the guardian. While during the digital KYC process, the digital thumb impression of the subscriber can also be accepted.

(G) The guardian and person with disability have to comply with the applicable KYC norms. The persons with disability may be classified as minor or major based on their age. Every person who has attained the age of eighteen years is considered as major and only a major, who is of sound mind and is not disqualified from contracting by any law is competent to enter into contract.

(H) The facility of all forms of permitted KYC can be extended to persons with disability by adopting accessibility standards. On request of the subscriber, the intermediary should extend their assistance for video capturing in live environment to facilitate online /video to persons with disability.

(I) The bank shall establish dedicated helplines for persons with disabilities, offering step-by-step assistance in completing the KYC process through voice or video support.

(J) Bank shall adhere to the following for compliance with Rule 9(1E) of the PML Rules, which states that the Bank that has last uploaded the subscriber's KYC records to CKYCR shall be responsible for verifying Customer Identification Procedures (CIP), including identity and address. Downloaded records by other Bank shall not require reverification of authenticity, provided they are current and compliant with PML Rules. Beyond identity/address, REs downloading and relying on CKYCR records remain ultimately responsible for maintaining the customer's economic profile, conducting risk assessment, and assigning risk categorization to ensure comprehensive CDD/EDD compliance as mentioned under section 2.2 of these guidelines.

42. 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-filing 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).

43. 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.

44. 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.

45. Collection of Account Payee Cheques

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

46. 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.

47. 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.

48. 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.

49. 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 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. Hiring of Employees and Employee training

- a. Adequate screening mechanism, including Know Your Employee / Staff Policy, as an integral part of their personnel recruitment/ 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 integrity 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.

56. 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.

57 Handling of exceptional cases in Non-KYC Compliant Accounts:

A menu Option “KYCRELAX” has been customized in CBS for allowing unfreezing as well as modifications of accounts in below mentioned exigencies/cases.

- Garnishee Order
- IT attachment
- Court Order
- Deceased Customer Cases

This menu option shall be exercised only by Circle Offices ZC users to ensure the discipline in respect of KYC Compliance.

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) FOR BASE BRANCHES

(A) For No Change in Customer Information:

- 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. Branch is required to seek the KYC Identifier from the customer or retrieve the same, if available, from the CKYCR and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, unless-
 - ❖ there is a change in the information of the customer as existing in the records of CKYCR; or
 - ❖ the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - ❖ the validity period of downloaded documents has lapsed; or
 - ❖ 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.
- e. The KYC documents/self-declaration obtained from customer shall be maintained alongwith Account Opening Form/Customer Master Form at the Base branch.
- f. 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 updation form, from the KYC updating branch, 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 to CKYCR portal in

terms of extant guidelines, where CKYC has not yet done.

(B) Change in Address:

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

- a. Branch is required to seek the KYC Identifier from the customer or retrieve the same, if available, from the CKYCR and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, unless-
 - ❖ there is a change in the information of the customer as existing in the records of CKYCR; or
 - ❖ the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - ❖ the validity period of downloaded documents has lapsed; or
 - ❖ 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.
- 2) 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.
- 3) 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.
- 4) The KYC documents/self-declaration obtained from customers shall be maintained along with Account Opening Form/Customer Master Form at the Base branch.
- 5) 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.
- 6) Branch shall ensure to upload the documents/ KYC details at CKYCR portal in terms of extant guidelines, where CKYC not yet done

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

(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 any 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 provide the CKYC Identifier from the customer or retrieve the same, if available, from the CKYCR

and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, unless-

- ❖ there is a change in the information of the customer as existing in the records of CKYCR; or
 - ❖ the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - ❖ the validity period of downloaded documents has lapsed; or
 - ❖ 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. 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 addresses 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.

(1.1.2) FOR NON-BASE BRANCHES

(A) For No Change in Customer Information:

- 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) Where KYC details available in CBS are not as per current CDD standard of KYC Policy of the Bank, branch is required to seek the KYC Identifier from the customer or retrieve the same, if available, from the CKYCR and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, 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. submit the requisite documents as per current CDD standards for KYC Updation.
- d) Branch shall update the KYC status and KYC Updation in CBS promptly.
- e) Branch shall upload the duly authenticated original copy of self-declaration/request received from the customer on the central depository (presently DMS) or send the same to the Base Branch and retain duly authenticated copy of the same as per extant record maintenance policy of the Bank.
- f) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

(B) Change in Address:

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

- a) For such cases, the Customer shall submit KYC documents or CKYC Identifier as per the current CDD standards by visiting at any branch.
- b) Branch on obtaining the KYC Identifier from the customer, shall retrieve the KYC records from the CKYCR by using such KYC Identifier and KYC Updation form the Customer and shall update the KYC details and KYC Updation date in CBS Promptly.
- c) Branch shall obtain the KYC documents as per current CDD standards for KYC

Updation where KYC Identifier is not available with the customer along with the KYC Updation form and shall update the KYC details and KYC Updation date in CBS Promptly.

- d) Branch shall upload the duly authenticated KYC documents/records received from the customer to the central depository (presently DMS) or to the Base Branch and retain duly authenticated copies 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.

(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 any branch, the same may be obtained from the customer through email-id registered with the Bank/ by post/ by letter/ 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) Where KYC details available in CBS are not as per current CDD standard of KYC Policy of the Bank, branch is required to seek the KYC Identifier from the customer or retrieve the same, if available, from the CKYCR and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, unless:
 - d) there is a change in the information of the customer as existing in the records of CKYCR; or
 - e) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - f) the validity period of downloaded documents has lapsed; or
 - g) 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. submit the requisite documents as per current CDD standards for KYC Updation.
- h) 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.
- i) On submission/verification by branch officials, the address shall be updated in CRM.
- j) 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.
- k) 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.
 - l) 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.
 - m) 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.
 - n) An acknowledgement of successful KYC updation shall be sent to Customer on his/her registered mobile no. through SMS.

1.2. **e-KYC authentication at any Branch**

- 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)

Eligible Customer

Customers whose KYC has been updated before 1 yr from current date are eligible.

Process Flow

- i. Customer will initiate the process by sending message '**KYCNC<Space> Customer ID last 4digit**' from his/her registered mobile no. with the Bank to 5607040/ 9264092640.
Note: Customers have to first save these no. (5607040/ 9264092640) on their mobile.
- ii. Customer will receive a message from Bank **<Your KYC request has been received. Kindly wait for some time while we process your request – PNB>**
- iii. The SMS/information will be sent on real-time basis through API to CBS for further processing.
- iv. CBS will then check for below mentioned validations-
 - Customer should not be a Minor.
 - Customer should be Resident Indian.
 - Tax Proof (PAN or Form 60) is available in CRM.
 - Customer should be a Retail customer with Low/Medium Risk.
 - Valid Aadhaar Number (ID Proof, Address Proof) is available in CRM.
 - Both Permanent and Communication address should be available in CRM.
 - KYC due date is less than or equal to 90 days from current date or KYC Updation is due.
 - Date of Birth, Gender, Profession/Activity, Father/Mother/Spouse Name (anyone), Residential status, Address, Annual Income, KYC Due date, CKYCR number is available in CIF ID.
 - All linked accounts are in active/unfreeze status.

Further, PAN validation and Aadhaar validation will also be carried out at Back End.

On successful validation, customer will receive message **<Customer ID in masked form xxxxxlast4digits> KYC is successfully done – PNB.**

Intermediary Message, if multiple messages are sent by the customer within a one-hour window, customer will receive message **Your KYC request has already been received. Kindly wait for some time while we process your existing KYC request – PNB**

In case of failure, customer will receive message **<Customer ID in masked form xxxxxlast4digits> KYC information is incomplete in your account. Kindly contact Branch with latest KYC documents to update your KYC – PNB.**

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

Eligible Customer

1. All customers whose KYC is due or going to be due in next 1 year.
2. Individual customers with mode of operation as "SELF".

Process Flow

1. Insert ATM Card.
2. Select “Other Services” ♦ “KYC Updation”
3. Enter ATM Pin
4. After correct entry of ATM Pin, customer will be prompted to confirm if there is any change in the KYC details. Once confirmation is given by customer as “No” i.e. there is no change in KYC details, customer will be shown a message on ATM Screen . ATM receipt shall also be generated.
5. The request is then sent to CBS for further validation as mentioned below:
 - Customer should not be a Minor.
 - Customer should be Resident Indian.
 - Tax Proof (PAN or Form 60) is available in CRM.
 - Customer should be a Retail customer with Low/Medium Risk.
 - Valid Aadhaar Number (ID Proof or Address Proof) is available in CRM.
 - Both Permanent and Communication address should be available in CRM.
 - KYC due date is less than or equal to 1 Year from current date or KYC updation is due.
 - Date of Birth, Gender, Profession/Activity, Father/Mother/Spouse Name (anyone), Residential status, Address, Absolute Income, KYC Due date, CKYCR number is available in CIF ID.
 - All linked accounts are in active/unfreeze status.

Further, PAN validation and Aadhaar validation will also be carried out at Back End.

On successful validation, customer will receive message **<Customer ID in masked form xxxxxlast4digits> KYC is successfully done – PNB**

In case of failure, customer will receive message **<Customer ID in masked form xxxxxlast4digits> KYC information is incomplete in your account. Kindly contact Branch with latest KYC documents to update your KYC – PNB.**

If KYC updation of customer is neither due nor falling due within 1 year, customer will receive message **“Dear Customer, your KYC updation is not due - PNB”**

Further, if customer selects “Yes” i.e. there is change in KYC details, customer will be shown a message on ATM Screen **<Please use other channels for submitting your latest KYC documents or contact your Branch>**

1.5. WhatsApp Banking (for no change in KYC Details)

Eligible Customer

Customers whose KYC has been updated before 1 yr from current date are eligible.

Process Flow

1. Send ‘Hi’ to 9264092640 on WhatsApp and follow the below path.

**All services → Account Related Services→ KYC Update
(OR)**

Simply type 'KYC'

2. Enter the OTP received on the registered mobile number.
3. All CIF IDs linked with the mobile number will be displayed in masked form.
4. Select the desired CIF ID.
5. Customer will receive a message from Bank **<Your KYC request has been received for customer ID <First two digits XXXX Last three digits>. Kindly wait for some time while we process your request – PNB>**

On successful validation, customer will receive WhatsApp message **<Customer ID First two digits XXXX Last three digits > KYC due date has been updated successfully**

Intermediary Message, if multiple messages are sent by the customer within a one-hour window, customer will receive message **Your KYC request has already been received. Kindly wait for some time while we process your existing KYC request – PNB**

In case of failure, customer will receive message **<Customer ID First two digits XXXX Last three digits > KYC information is incomplete in your account/ validations failed. Kindly contact Branch with latest KYC documents to update your KYC – PNB**

Further, if KYC updation of customer is neither due nor falling due within 1 year, customer will receive message **Dear Customer, your KYC is valid up to DD-MM-YYYY. Kindly update 1 year before expiry**

1.6. IBS/MBS/Corporate Website of the Bank

a) Portal Access and Authentication Journey:

- (i) Customer will login into IBS/MBS or visit Bank's corporate website. A link is available in IBS, MBS, Bank's corporate website that redirects the customer to KYC Updation portal.

Path for all three channels are as under:

- **IBS- Post Login** → Personal Settings → Check KYC Status → KYC Update Details
- **MBS- Post Login** → Profile Settings → Check KYC Status → Update KYC
- **Corporate website** → Online Services → Digital KYC Updation

- (ii) Customer will enter his CIF ID and receive OTP on his/her registered mobile number. CIF ID can be checked from Passbook/ Account Statement / Internet Banking/ PNB One.
- (iii) Customer will enter the OTP for validation.
- (iv) Once the OTP is Validated, system checks for the following validations:
 - a. Customer is not minor.
 - b. Customer is resident Indian.
 - c. Customer is Retail customer with Low/Medium Risk.
 - d. Permanent address is available in CRM.

- e. Date of Birth is available in CRM.
- f. Gender is available in CRM.
- g. Father/Mother/Spouse Name (anyone) is available in CRM.
- h. KYC due date is available in CRM and last KYC updation date is not less than 30 days from the current date.
- i. If invalid/ blank value is present in Absolute income field, then Highest value of income present in Income slab is derived as Absolute Income (upto 15 lakhs else not eligible).
- j. All linked accounts are in active/unfreeze status.
- k. Valid Aadhaar Number (ID Proof/Address Proof) is available in CRM.
- l. Tax Proof (PAN or Form 60) is available in CRM
- m. Dedupe check (Multiple CIF IDs)

In case of failure of any of the above validations, appropriate message is displayed to the customer on screen and KYC is not updated through IBS, PNB One or Corporate website.

- (v) After successful validation, following details are displayed to customer in non-editable form:
- a. Full Name
 - b. Father/ Mother/ Spouse name (whichever is available in CBS)
 - c. Date of Birth
 - d. Gender
 - e. Profession/Activity
 - f. Annual Income
 - g. Physical state (Non-disabled / Differently abled)
 - h. Tax Proof (PAN/Form 60) (Masked Form)
 - i. OVD (Masked form)
 - j. CKYCR Number (Masked form)
 - k. Address (Present and Communication)

- (vi) The customer is provided with two options:

- No change in KYC Information
- Change in KYC Information

b) Workflow for "No change in KYC Information"

- (i) If customer selects no change in KYC information, system checks that following fields are available in CRM:
- Both permanent and communication address
 - Profession/Activity
 - CKYC number
 - Physical state (Non-disabled/ Differently abled)
- Note- If Physical state (Non-disabled/ Differently abled) or CKYC Number is not available in CBS, then customer will be informed to continue the journey under "Change in KYC details"
- (ii) Customer confirms that there is no change in his/her KYC details.
- (iii) System displays message on screen "Your request for KYC updation is under process. Kindly wait for some time"

- (iv) If successful response is received, Message will be displayed on screen "Your KYC has been updated successfully"
- (v) KYC date will be updated in CBS.
- (vi) If response is unsuccessful, Message to be displayed on screen "Your KYC has not been updated successfully, Kindly visit Bank's Branch".

Note: Since the customer's CKYC number is already available in the system and there has been no change in the customer's KYC details, there is no requirement to re-upload the customer's KYC data to CKYCR.

c) Workflow for "Change in KYC Information"

- (i) If customer selects "Yes" under "Do you want to change any of the above KYC details", CKYCR Search will be done on CKYCR Number/PAN/OVD in the background. PAN Validation, Aadhaar Validation (only if Aadhaar in non-eKYC form), AML Check, will also be carried out in back end.
- (ii) Customer shall be provided with the facility to modify the following details:
 - a) PAN (If Form 60 is available in CRM)
 - b) Profession/ Activity
 - c) Income
 - d) Communication Address
- (iii) Profession/Income will be self-declared by choosing from different profession/activity available through drop down.
- (iv) Income will be manually entered by the customer.
 - a) If entered income is upto the limit as specified by the Bank from time to time – Income will be accepted on self-declaration on final preview page.
 - b) If entered income is more than the limit as specified by the Bank from time to time - Income will be verified through Income Tax Website for which customer has to enter his/her income tax portal password.
- (v) If customer's Physical state (Non-disabled/ Differently abled) field is not available in CBS, then customer will be asked to fill the details mandatorily.
 - a. Customer may select non-disabled or differently abled from the drop down.
 - b. If customer selects differently abled, then following details are mandatorily required to be filled by the customer: -
 - i. Type of Disability
 - ii. Nature of Disability
 - iii. Percentage of disability
 - iv. UDID Number
- (vi) Customer may update his/her address as per information available in Aadhaar or CKYCR. Same will be validated through Aadhaar OTP or OTP received from CKYCR. Documents from CKYCR will be validated through Optical Character Reader (OCR).
- (vii) In case PAN is entered by customer, same will be verified through PAN validation. Further, existing PAN will also be validated.
- (viii) After modifying the necessary details, final preview will be displayed to the customer for checking the details.
- (ix) On successful validation, updated details along with KYC Updation date will flow to CBS and CERSAI for CKYC purpose. Customer will also receive an SMS on

registered mobile no. "Your KYC has been updated successfully".

- (x) If response is unsuccessful, customer will receive an SMS on registered mobile no. "Your KYC has not been updated successfully, Kindly visit Bank's Branch".

2. ACCOUNTS OF CUSTOMER, WHO WERE MINOR AT THE TIME OF OPENING ACCOUNT, 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 shall be 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)

The following are the modes in VCIP:

- (iv) **Assisted VCIP with Human Officer Review:** An official of the RE conducts a live video call with the subscriber to verify their identity. The official guides the subscriber through the process, ensuring real-time interaction and document verification.
- (v) **Unassisted VCIP (Self-Service Video KYC):** The subscriber completes the KYC process independently via a secure video-based platform or app, without direct human interaction, using automated systems for verification.
- (vi) **Hybrid VCIP (Combination of Assisted and Automated Verification):** Combines elements of assisted and unassisted VCIP, where automated systems handle initial verification, and a human officer intervenes for final review or complex cases.

Further, the facility of online / digital / Video Based Customer Identification Process also to be extended to persons with disability by adopting accessibility standards. On request of the subscriber, the RE shall extend their assistance for video capturing in live environment to facilitate online /Video for persons with disability.

For the purpose of 'liveliness' check, intermediaries may use various parameters which not only involves checking the movement of eyelid and eyeball or blinking, but also may use other factors viz live facial expressions, nodding of head, subscriber showing OTP while being clearly visible on-screen, real-time video recording and displaying copies of documents on the screen etc. Where a subscriber is unable to perform OTP-based or expression-based checks, the RE shall provide alternative authentication methods, such as:

- (iii) **Document-based OVD verification with live photo capture.**
- (iv) **Use of CKYCR/ UIDAI/ DigiLocker records for identity confirmation.**

The liveliness check shall not result in exclusion of person with special needs and at the same time the accessibility options shall not dilute liveness/integrity checks under PML Rules.; Or

(a) In case of digital onboarding for the NRI/OCI subscribers, the requirement of capturing a live photograph of the subscribers, a digital copy of an officially valid document (OVD) and geo-coordinates of the captured location, all recorded electronically by an authorized official shall be applicable. For this purpose, the requirement of physical location of subscriber being in India, during digital onboarding, shall be relaxed for KYC for the subscriber.

(b) The Points of Presence (PoPs) shall ensure that the GPS location

(latitude and longitude) captured by the intermediary matches with the latitude and longitude of country given in Proof of Address of the subscriber and it shall also prevent connections from spoofed IP address. The digital onboarding application shall incorporate liveness detection, randomness checks, and anti-spoofing/anti-deep fake measures, ensuring that the interaction is live, tamper-proof and not pre-recorded.

- f) By “using Digilocker” as prescribed by the PFRDA vide circular no. PFRDA/2021/5/PDES/5 dated 3rd February 2021 (Annexure 3) Or;
- g) Where the subscriber is an existing customer of the bank, acting as PoP, the KYC records maintained in the bank’s core banking system (CBS) may be used for NPS onboarding, provided that such records are originally obtained in compliance to the Prevention of Money Laundering Act (PMLA), and the extant Master Directions of RBI as amended from time to time. PoPs shall ensure that such KYC records are valid, updated, fall within the prescribed periodic updation cycle, and meet the requirements applicable for opening an NPS account under these guidelines. Further, PoP shall require the subscriber to re-confirm the correctness and completeness of such KYC information through OTP based authentication. PoPs shall maintain audit trail including consent records and make them available to the relevant authorities during inspection.; Or
- h) For the purpose of KYC, PoPs may also rely on third party KYC related to the subscribers as mentioned under section 12 of these guidelines.
- i) By using "KYC identifier" allotted to the subscriber by the CKYCR Or

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

Note: Bank shall establish a mechanism for human review of rejected KYC applications in cases where accessibility-related challenges prevent successful verification. No application for onboarding or periodic updation of KYC for persons with disabilities shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

ML/TF Risk Assessment

- a. Source of contribution
- b. Mode of contribution (Cash / Online / Cheque / DD / Card / employers bank account etc.)
- c. Regularity in the flow of contribution (For eg - Contributions under employer and employee relationship)
- d. Withdrawals under Tier I and Tier II account under All Citizen Model/Corporate Model or any other scheme as may be approved by PFRDA from time to time.

- e. Residence status of subscriber (For eg - Subscribers residing in jurisdiction with higher national risk assessment)
- f. 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 photograph of 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 is available, 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 the document.; 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 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
loResponse :
- 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 frozen 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.

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

Annexure-IV

KYC documents for eligible FPIs under PIS

Document Type		FPI 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 *

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

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 over 25%”)	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 of opening bank accounts, etc., is not in vogue, may submit 'Power of Attorney granted to Global Custodian / Local Custodian in lieu of Board Resolution'				

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

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 Know Your Customer (KYC)?

Response: KYC is an acronym for "Know your Customer". It is a term used for Customer identification process by which a bank, obtains information about identity and address of the customer, nature of business and financial status of a customer and verifies the same 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. This process helps to ensure that bank is aware of the customer it is dealing with, and the services provided by the bank is not misused for Money Laundering/ Terrorist Financing/ Proliferation Financing (ML/TF/PF) purposes.

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. Is KYC mandatory? When a bank is required to carry out KYC?

Response: Yes, KYC is mandatorily required to be carried out:

- at the time of commencement of an account-based relationship, i.e., opening any type of account with the bank; or
- when a walk-in-customer carries out occasional transaction of an amount equal to or exceeding ₹50,000 (whether conducted as a single transaction or several transactions that appear to be connected); or
- when a walk-in-customer carries out any international money transfer operations; or
- when the bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained; or
- when the bank sells its own products or third party products as an agent; payment of dues of credit cards/ sale and reloading of prepaid/ travel cards and any other product for more than ₹50,000.

Q 3. Who is a walk-in-customer?

Response: A "Walk-in Customer" means a person who does not have an account-based relationship with the bank but undertakes transactions with the bank.

Q 4. Does a customer have to furnish KYC documents for each account he opens with the same bank?

Response: No, if an existing KYC compliant customer of a bank desires to open another account or avail any other product/ service from the same bank, he is not required to submit any KYC document unless there is a change in the information with respect to his identity and/ or address. 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 5. What is a ‘Small Account’?

Response: In case a customer does not possess an OVD, he can still open a ‘Small Account’ with a bank. For the purpose, the bank shall obtain a self-attested photograph from the customer and 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. The Small Account shall remain operational initially for a period of twelve months and is subject to conditions as given under paragraph 5 of the KYC Policy.

Q 6. What are deemed OVDs for the purpose of proof of address?

Response: The customer can furnish one of the following documents or the equivalent e- documents thereof, if the OVD submitted by him to the RE does not contain current address. These documents are **deemed to be OVDs** for the limited purpose of proof of address:

- a. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- b. property or Municipal tax receipt;
- c. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- d. 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 licence agreements with such employers allotting official accommodation.

However, the customer shall submit OVD with current address within a period of three months of submitting the document specified above.

Q 7. If a customer is staying, say, in Chennai but his OVD contains the address of, say, New Delhi, can he open an account in Chennai?

Response: Yes. The customer can open an account with a bank by submitting a *deemed to be OVD* for the purpose of proof of address. However, as mentioned in reply to **Q 6** above, he is required to submit OVD with current address within a period of three months.

Q 8. If there is a change in the name and the OVD does not include the new name, how can one open an account?

Response: In such case, an OVD containing the earlier name along with a copy of the Gazette notification, or marriage certificate issued by the State Government, as applicable, indicating the change in name, can be submitted for

opening the account.

Q 9. Is fresh KYC needed where a customer transfers his existing account from one branch office of the bank 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, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Q 10. Whether KYC is required to be done for all account holders of a joint account?

Response: Yes, documents as mentioned in reply to Q 6 above shall be submitted by all account holders of a joint account to the bank.

Q 11. What are the different modes for onboarding individual customers by the bank?

Response: Bank has the following options to onboard a customer:

(a) Face-to-face onboarding:

- Visit to the branch office of the bank;
- using e-KYC authentication (OTP as well as biometric based authentication); undertaking offline verification of proof of possession of Aadhaar Number; obtaining certified copy of the OVD or equivalent e-document thereof; undertaking 'Digital KYC Process', as per Annexure II of the KYC Policy.
- Video based Customer Identification Process (V-CIP) complying with prescribed standards and procedures.

(b) Non-face-to-face onboarding:

- using Aadhaar OTP based e-KYC authentication;
- using digital channels such as CKYCR, DigiLocker, 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^[1].

[1]. The Person of Indian Origin (PIO) card scheme was withdrawn and merged with the Overseas Citizen of India (OCI) card scheme via Gazette Notification No. 25024/9/2014-F.I on 09.01.2015. Hence "PIO" may be treated as "OCI".

Q 12. What is a KYC Identifier? How is it useful for a customer?

Response: KYC Identifier means the unique number or code assigned to a customer of a bank by the Central KYC Records Registry (CKYCR). If the customer approaches a bank for opening an account, he can provide his KYC Identifier and give consent to the bank to download the valid KYC data from CKYCR. This can obviate the need for the customer to submit KYC documents again while opening an account with the Bank.

Q 13. Can the KYC Identifier be used for any other purpose?

Response: In addition to the purpose of establishing an account-based relationship, KYC Identifier can be used for updation/ periodic updation of KYC, or for verification of identity of a customer. Further details in this regard are given

in paragraph 40(j) of the KYC Policy.

Q 14. Whether customers’ consent is required for opening of account using KYC identifier?

Response: Yes, the bank is required to obtain customer’s explicit consent to use his/ her KYC Identifier for downloading KYC records from CKYCR for the purposes mentioned in response to Q. 14 and 15.

Q 15. How can a customer obtain his KYC Identifier issued by CKYCR?

Response: A customer can obtain his KYC Identifier through the following ways:

- a. In the process of opening an account, once the customer’s KYC Identifier is generated by CKYCR and provided to the bank, the latter shall share the same with the concerned customer.
- b. The customer can also access his KYC Identifier on CKYCR Portal (www.ckycindia.in).

Q 16. It is easy to use KYC Identifier for opening an account. Whether any measure has been taken to improve its use by the banks?

Response: For the purpose of opening an account, bank is required to seek the KYC Identifier from the customer or retrieve the same, if available, from the CKYCR and obtain KYC records by using such KYC Identifier. In such cases, the customer is not required to submit the same KYC records/ information/ any other additional identification documents, unless—

- a. there is a change in the information of the customer as existing in the records of CKYCR; or
- b. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
- c. the validity period of downloaded documents has lapsed; or
- d. 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.

Q 17. What is Video-based Customer Identification Process (V-CIP)?

Response: V-CIP is an alternate method of customer identification with facial recognition and customer due diligence that allows the bank to obtain and verify a customer’s identity information through a digital, secure, live, informed and consent-based and live audio- visual interaction between an authorised bank official and the customer to obtain identification information required for CDD purpose. V-CIP eliminates the need for physical visit to a branch of the bank but is treated on par with face-to-face CIP. Assisted V-CIP is also permitted when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end.

Q 18. Whether blinking of eyes or making specific facial gestures are mandatory to complete V-CIP?

Ans: No, making specific facial gesture like blinking of eyes, smiling, frowning, etc.

are not mandatory for liveness check. The bank is required to take due cognizance of special need, if any, of the customer during liveness check.

Q 19. What are the purposes for which V-CIP can be used by a bank?

Response: V-CIP may be used for carrying out the following processes:

- a. to undertake CDD in case of onboarding a new individual customer, proprietor in case of proprietorship firm, authorised signatories and beneficial owners in case of Legal Entity customers;
- b. to convert existing account opened in non-face-to-face mode using Aadhaar OTP based e-KYC authentication; and
- c. for updation/ periodic updation of KYC records of eligible customers.

Q 20. Why does the bank periodically ask for KYC documents from the customer when the customer has already submitted the same during opening of account?

Response: Bank is required to update the customers' KYC records as part of ongoing due diligence process to ensure that the information or data collected under CDD is kept up to date and relevant. The periodicity of such updation depends on the risk categorisation of the customer by the bank and such periodic updation of KYC records (*at times referred to as re-KYC*) shall be carried out at least once in every two years for high-risk, eight years for medium risk and ten years for low-risk customers. However, Bank may adopt any additional and exceptional measures as per its internal KYC policy which *inter alia* may require physical presence of the customer, periodic updation of KYC only in the branch of the RE where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity, etc.

Q 21. What are the parameters used by the bank for risk categorisation of a customer?

Response : The broad indicative parameters prescribed for customer's risk categorisation are customer's identity, social/ financial status, nature of business activity, information about the customer's business and his/ her location, geographical risk covering customer 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. The risk category and reasons thereof are not required to be divulged to the customers by the bank.

Bank has issued detailed guidelines for “Risk Categorization of Customers” vide DPMD Cir No. /2025 dated 20.04.2025.

Q 22. *What are the modes for periodic updation of KYC for individual customers?

Response: The modes for periodic updation of KYC for individuals are as under:
a. It can be undertaken at the branch of the bank with which customer maintains

- the account or any other branch of the bank; or
- b. Bank can obtain a self-declaration when there is “no change in KYC information” and also when there is “change only in address details”, through customer’s email-id/ mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of the bank), letter, etc. However, the declared address shall be verified by the bank through positive confirmation within two months; or
 - c. Aadhaar OTP based e-KYC in non-face-to-face (NF2F) mode and V-CIP;
 - d. Bank is also mandated to update customer’s KYC records based on the update information/ notification, if any, received from CKYCR for the customer concerned.

Q 23. What documents are needed for periodic updation of KYC?

Response: The requirement of KYC documents depends on the modes used for periodic updation of KYC as detailed in the reply to Q 24, above.

- a. In case of change in the KYC information, the customer has to provide the documents as mentioned in the reply to Q 5 above;
- b. In case of no change in KYC information, the customer can provide a self-declaration. Similarly, a self-declaration in case of change only in address can also be provided by the customer to bank as detailed in reply to Q 24 above.
- c. In case of Aadhaar OTP-based e-KYC authentication facility in non-face-to-face mode, the customer can provide a declaration of the current address even if the current address is different from the address in Aadhaar database. However, bank shall ensure that mobile number for Aadhaar authentication is same as the one available with it in the customer’s profile, in order to prevent any fraud.
- d. In case of use of V-CIP for completing re-KYC, the requirements shall be as per paragraph 4 of the KYC Policy, which include identification and verification of the identity using (i) Aadhaar OTP based e-KYC authentication in non-face-to-face mode; (ii) offline verification of Aadhaar; (iii) KYC records downloaded from CKYCR; and (iv) equivalent e-documents including documents issued through DigiLocker.

Q 24. Can the customer get an acknowledgment from the bank after submitting the KYC documents for periodic updation of KYC?

Response: Yes, once a customer submits updated KYC information or self-declaration to the bank, it shall provide an acknowledgement to this effect to the customer. Upon updating KYC information, the bank shall also intimate customers about such updation.

Q 25. Is the Bank required to give due notices to the customer for completing his pending periodic updation of KYC?

Response: Yes, the Bank shall intimate its customer, in advance, to comply with the requirement of periodic updation of KYC. Subsequent to the due date, Bank shall also give reminders to such customer who has still not complied with the requirements, despite advance intimations.

Q 26. What happens if periodic updation of KYC is not done even after advance intimations/ reminders?

Response: Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 enable the Bank to obtain the identity records (including updated records of identity) from the customers, failing which the bank shall close the account of the customers after giving due notice.

Q 27. What should a customer do if he receives SMS/ email with links to complete periodic updation of KYC?

Response: The customer shall exercise **utmost caution** before clicking links embedded in such SMS/ email as these may be suspicious/ fraudulent. The public is advised not to fall prey to frauds being perpetrated in the name of KYC updation.

Q 28. Can a person purchase a Demand Draft/ Payment Order/ Travellers Cheque against cash?

Response: Demand Draft/ Payment Order/ Travellers Cheques for amount less than ₹50,000 can be purchased against cash. However, such instrument for ₹50,000 and above can be issued only by way of debiting the customer's account or against cheques.

Q 29. What is the period of presenting payment instruments including cheques/ drafts/ pay orders/ banker's cheques?

Response: Payment of cheque/ draft/ pay order/ banker's cheque, if presented beyond the period of three months from the date of issuance of such instrument, shall not be made by bank.

Q 30. What should a customer do in case the documents submitted by the customer, at the time of establishing an account-based relationship (opening an account with bank), have been modified/ updated/ renewed?

Response : In case of any change in the OVDs such as change in demographic information or address or other documents submitted by a customer at the time of establishing account- based relationship, the customer shall submit the updated OVD/ other documents to the bank within 30 days of the update/ change/ modification in the documents for the purpose of updating the records at bank's end. In such case, the bank shall acknowledge the receipt of the KYC documents to the customer.

Q 31. Whether all modes of customer onboarding (i.e., opening of account) as mentioned in the reply to Q 13 are available to the person with disabilities (PwD)? **Ans:** Yes, all modes of account opening as mentioned in the reply to Q 13 above, viz. onboarding customer in face-to-face mode; non-face-to-face mode and V-CIP are available to the person with disabilities.

Q 32. Whether the application of KYC/ periodic updation of KYC of a

customer can be rejected automatically?

Response: Banks' 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, including the persons with disabilities (PWDs). The decision to reject the application of KYC/ periodic updation of KYC shall not be automated and such decisions on rejection shall be reviewed by an official of bank authorised for the purpose.

Q 33. Whether thumb impression in place of signature would be accepted for KYC purposes?

Ans: The provision to accept thumb impression in place of signatures has already been prescribed for onboarding customer in face-to-face-mode under paragraph 2 and 5 of the KYC Policy.

Q 34. *What is an inoperative account¹? What is the procedure for reactivating an inoperative account?

Response: Inoperative Account is a savings/ current account wherein no 'customer induced transactions' has taken place for a period of over two years. For activation of inoperative accounts, the customer can update his/ her KYC information/ data at home/ non-home branch of the bank, and also through V-CIP, subject to the facility of V-CIP being provided by the bank. The banks shall activate the inoperative accounts, only after adhering to the KYC guidelines provided in the KYC Policy.

Q 35. What are the modes through which inoperative accounts can be made operational?

Ans: To ease the process of activating the 'Inoperative Accounts', bank has made available the facility of updation of KYC at all branches of the bank, through Video- Customer Identification Process (V-CIP) if requested by an account holder.

Q 36. 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 37. 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 Reserve Bank of India (Commercial Banks – Know Your Customer) Directions, enforces legal/statutory/regulatory obligations on both bank and customers to provide KYC information/documents.

Q 38. 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 39. 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 40. What are the documents to be obtained from customers as 'proof of identity' 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 specified in the KYC policy.

Q 41. 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 42. 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 43. 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 44. If customer does not have any of the documents listed above to show his/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 45. 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 46. If customer refuses to provide requested documents for KYC to the bank for 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 47. 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 48. Is Aadhaar mandatory for opening of an account?

Response: No. However, in case the customer 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), the customer **shall** provide the Aadhaar number and is required to undertake Aadhaar authentication using e-KYC facility of UIDAI. In other cases, the Aadhaar number **may** be provided voluntarily by the customers.

Q 49. 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 authentication to 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 50. Is introduction necessary while opening a bank account?
Response: No, introduction is not required.

Q 51. 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 52. 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 53. 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)^[4], 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-resident customer resides.

[4]. The Person of Indian Origin (PIO) card scheme was withdrawn and merged with the Overseas Citizen of India (OCI) card scheme via Gazette Notification No. 25024/9/2014-F.I on 09.01.2015. Hence "PIO" may be treated as "OCI".

Q 54. What are the documents required for opening a bank account by an individual?

Response: Following documents are required for opening of an account by an individual:

any one of the following Officially Valid Documents (OVDs) or the equivalent e-document thereof, containing details of his name and address, viz.,

- the passport,
 - the driving license,
 - proof of possession of Aadhaar number,
 - the Voter's Identity Card issued by the Election Commission of India,
 - the job card issued by NREGA duly signed by an officer of the State Government, and
 - the letter issued by the National Population Register.
- (b) the Permanent Account Number (PAN) or the equivalent e-document, thereof, or Form No. 60 as defined in Income-tax Rules, 1962; and
- (c) other documents 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.

Q 55. 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 56. What documents are required for opening an account of trust (registered)?

Response: For opening an account of a trust (registered), certified copies of each of 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 57. 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 58. 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 59. 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 60. 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 verify the 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 61. 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 62. 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 63. 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 64. What KYC documents are required to open account of a Nepali Citizen?

Response: Extant KYC Policy of Bank which is in line with Reserve Bank of India (Commercial Banks – Know Your Customer) Directions 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.

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

Appendix - 1

Oversight responsibilities of the Board/ Committees of the Board

S. N.	Board/ Committee of the Board	Details of Oversight responsibilities	Subject/ Title of the agenda note to be placed	Division responsible for placing the note	Periodicity of review
1	Audit Committee of Board	Review of implementation of Know Your Customer (KYC) guidelines.	Review of implementation of Know Your Customer (KYC) guidelines.	Data Privacy & Management Division	Quarterly

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

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

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- Governmental 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

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

“Confidential
Strictly for internal Circulation Only”

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

CHAPTER B

(Part-I Policy)

Policy for Anti Money Laundering (AML)- Combating the Financing of Terrorism (CFT) and Know Your Customer (KYC) of PNB BO: IFSCA Banking Unit (IBU), GIFT City, Gujarat

(As per IFSCA Guidelines dated 17.11.2025 and
Circulars issued up to 05.01.2026)

Office : PNB BO: IBU GIFT City
Division : Data Privacy & Management Division
Version : 2026_AML/CFT/KYC (GIFT City) _1.0

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*"Confidential
Strictly for internal Circulation Only"*



Policy Custodian

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

Policy Version Control

S. No.	Version Number	Version Date	Summary of changes
1	2021_IBD_1.0	27.01.22	New Policy
2	2023_AML (GIFT City)_1.0	28.06.23	Present Policy is prepared as per New IFSCA AML-CFT and KYC guidelines dated 28.10.2022
3	2024_AML(GIFT City)_1.0	29.05.24	(Present Policy is prepared as per New IFSCA AML-CFT and KYC guidelines dated 28.10.2022)
4.	2025_AML(GIFT City)_1.0	30.04.25	IFSCA Guidelines dated 17.11.2025 and Circulars issued up to 05.01.2026.
5	2026_AML (GIFT City)_1.0		Present Policy is prepared as per New IFSCA AML-CFT and KYC guidelines dated 17.11.2025.

Policy Governance

Frequency of Review	Annual
Last reviewed on	30.04.2025
Approval Path	ACE> ACB > Board
Supersedes	2025_AML (Gift City)1.0

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

Contents

Sr. No.	Particulars	Page No.
	(Part-I Policy)	
1.	Policy Overview	171
2.	Policy Details	171
2.1	Background	171
2.2	Objective and Purpose	171-172
2.3	Scope and Applicability	172
2.4	Policy Contents	172-173
2.5	Authority for approving Operational Guidelines	176
2.6	Disclosure of Policy	176
2.7	Ownership of Policy	176
2.8	Validity and Review of the Policy	176
2.9	Reporting	176
2.10	Exclusions	177
	(Part- II Operational Guidelines)	
1.	Definitions	180-187
2.	Risk Based Approach	187-188
3.	Business Risk Assessment	189
3.1	Identifying and assessing business AML Risks	189
3.2	New Products, business practices and technologies	189-190
3.3	AML/CFT systems and controls	190-191
4.	Customer Risk Assessment	191
4.1	Assessing customer AML risks	191
4.2	Factors that may indicate high ML/TF risk	192-193
4.3	Factors that may indicate low ML/TF risks	193-194
4.4	Cases where Business relationship should not be established.	194-195
5.	Customer Due Diligence	195
5.1	Customer Due Diligence Process	195
5.2	Timing of CDD	195
5.3	Establishing business relationship before verification	195-197
5.4	Customer Due Diligence Requirement	197-205
5.5	Accounts of Politically Exposed Persons	205-207
5.6	Enhanced Due Diligence	207-209
5.7	Simplified Due Diligence	209-210
5.8	Ongoing Customer Due Diligence	210-211
5.9	Ongoing Sanctions Screening	211
5.10	Failure of Regulated Entity to conduct or complete customer due diligence	211-212
5.11	Periodic Updation	212-214
6.	Third Party Reliance	214-216
7.	Correspondent Banking and Wire Transfer	216
7.1	Correspondent Banking	216-217

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

7.2-7.6	Wire Transfer	217-218
7.7-7.9	Responsibility of the Ordering, Beneficiary and Intermediary Institution	218-221
8	Internal Policies, Compliance, Audit and Training	221
8.1	Internal Policies	221
8.2	Compliance	221-222
8.3	Audit	222-223
8.4	Training and awareness	223-224
9.	Record Keeping	224-226
10.	Process of Identification of suspicious Transactions	226
10.1	Internal Reporting requirements	226
10.2	Indications of Suspicious Transactions	226-229
10.3	Reporting of Suspicious Transactions	229-230
10.4	Confidentiality of Suspicious Transaction Report	230-231
10.5	Additional Measures	231-232
11.	Compliance obligations under international agreements and domestic laws	232
11.1	Requirements/obligations under International Agreements Communications from International Agencies	232-233
11.2	Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967	233
11.3	<u>Obligations under Weapons of Mass Destruction (WMD)</u>	233
11.4	Jurisdictions that do not or insufficiently apply the FATF Recommendations	234
11.5	Secrecy Obligations and Sharing of Information	234
11.6	Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)	234-235
11.7	Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR)	235-237
12	Validity and Review of the Operational Guidelines	237
Annexure-I	Guidance on CDD Procedure	238-243
Annexure-II	V-CIP process for on-boarding Indian nationals	244-251
Annexure-III	Index of abbreviations	252
Annexure -IV	AML risk identification and client risk allocation document (customer risk assessment template)	253-257
Annexure - V	Frequently Asked Questions (FAQs)	258-272
Appendix - 1	Oversight responsibilities of the Board/ Committees of the Board/ Functional Committee	273

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, PNB BO: IBU GIFT City, Gujarat 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 AML- CFT and KYC Policy is issued for the branch in terms of International Financial Services Centres Authority (Anti Money Laundering, Counter- Terrorist Financing and Know Your Customer) Guidelines, 2022 dated 17.11.2025 and Circulars issued up to 05.01.2026.

2. POLICY DETAILS

2.1 BACKGROUND

AML- CFT and KYC Policy of PNB BO: IBU GIFT City, Gujarat was last approved by the Board in its meeting held on 30.04.2025 as per IFSCA AML-CFT and KYC Guidelines, 2022 dated October 28, 2022 and Gazette notification CG-DL-E-07032023-244194, CG-DL-E-03052023-245631, CG-DL-E-09052023-245764.

2.2 OBJECTIVE 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 the 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. This policy has been framed to develop a strong mechanism for achieving the following objectives:

- (i) To prevent the Branch from being used intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Branch to know/understand its customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.
- (ii) To enable the Branch 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 this 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 & APPLICABILITY

2.3.1 The provisions of these Guidelines shall apply to IFSC Banking Unit (IBU) of Punjab National Bank at GIFT City, Gujarat, which has been granted license by International Financial Services Centres Authority (IFSCA). The Branch shall take all necessary steps to implement this 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, by the Government of India including operational instructions issued in pursuance of such amendment (s).

2.3.2 In case there is a variance in AML- CFT and KYC standards prescribed by the Reserve Bank of India (RBI) and IFSCA, the Branch is required to adopt the more stringent regulation of the two.

2.4 POLICY CONTENTS

THE AML-CFT AND KYC POLICY INCLUDES FOLLOWING KEY ELEMENTS: -

2.4.1 RISK BASED APPROACH

The primary thrust of these Guidelines is to enable the Branch to adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which the Branch is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc., and document the same.

(i) Business Risk Assessment

The Branch shall take into consideration the nature, size and the complexity of its Business Activities and take suitable steps to identify its exposure to ML/ TF risks.

(ii) Customer Risk Assessment

Risks identified while assessing the business risks shall be used for the customer risk assessment. The customer risk assessment shall be performed while taking into

consideration the parameters, or the process as specified in Operational Guidelines Part-II. The outcome of the Customer risk assessment shall be used to assign the risk rating of the customer as high, medium or low, proportionate to the ML/TF risks.

The result of the risk assessment shall be used to classify the ML/TF risks as Low, Medium, High. To keep the risk assessments up-to-date, the Branch shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Governing Body. While assessing the risk factors, the Branch shall examine the overall risk, keeping in mind that the presence of one or more risk factors alone may not always indicate a high or low risk of ML/TF in a particular situation. The RBA should be an essential foundation in Branch's AML-CFT compliance culture, and it must trickle down from the level of Senior Management to the rest of the organization. The AML/CFT policies, procedures and controls shall be approved by Senior Management to enable the Branch to effectively manage and mitigate the risks either identified by it or notified to it by the Authority or other relevant authorities. Further, the Branch shall constantly monitor the implementation of RBA and improve if necessary.

2.4.2 CUSTOMER DUE DILIGENCE

- (i) The Branch shall not establish the business relationship with the customer, where the ownership or control arrangements of the customer prevent the Branch from identifying one or more of the customer's Beneficial Owners, where there are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the Branch or a Shell Financial Institution.
- (ii) The Branch, after assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the customer due diligence. It shall identify the customer and the beneficial owner and verify their identity. It shall conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Branch's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.
- (iii) The branch shall review its customers, their business and transactions against United Nations Security Council Sanctions lists and also against any other relevant sanctions list while conducting ongoing due diligence.

2.4.3 COMPLIANCE OF THE POLICY

Compliance of this policy, as advised in IFSCA Guidelines on AML, CFT and KYC will be ensured as under-

(a) **DESIGNATED DIRECTOR**

- (i) The Chief Executive Officer of the Branch shall be the "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, the Rules and these Guidelines.
- (ii) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
- (iii) In no case, the Principal Officer be nominated as the 'Designated Director'.

(b) **PRINCIPAL OFFICER**

- (vii) Compliance Officer at Branch, minimum in the rank of Scale- IV, shall be the Principal Officer of the Branch for the purpose of this policy, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under rule 8 of the Rules and the law / regulations.
- (viii) To enable unbiased judgements and facilitate impartial advice to management, the Principal Officer shall be distinct from the internal audit and business line functions.
- (ix) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- (x) The Principal Officer shall report to Senior Management on the outcome of reviews of the Branch's compliance with these Guidelines & risk assessment procedures.

(c) **COMPLIANCE MECHANISM**

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

- (i) Senior Management as defined in Governance Framework Policy for the Branch.
- (ii) Allocation of responsibility through Office Order for effective implementation of policies and procedures at Branch level.
- (iii) Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Compliance Division, HO.
- (iv) 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.
- (v) At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML/CFT guidelines at the branch would be reviewed for apprising Audit Committee of Board.

- B. It is to be ensured that decision-making functions of determining compliance with KYC norms are not outsourced by the branch.
- C. PML Rules require the Branch 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-
2. be documented;
 3. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
 4. be kept up to date; and
 5. be available to competent authorities and self-regulating bodies.
- D. The implementation of KYC-AML/CFT guidelines by the branch in letter and spirit, are to be ensured by the Governing Body, i.e., the committee constituted as per Governance Framework Policy for the Branch.
- E. **Designated Director and Principal Officer under the Guidelines shall mandatorily undergo the certification course namely “NISM-IFSCA-01: Certification Course on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) in the IFSC” developed by the National Institute of Securities Markets (NISM) in collaboration with the IFSCA Academy and they shall continue to hold the said certification at all times while discharging their responsibilities under the Guidelines. Apart from the Designated Director and Principal Officer, other employees of PNB IBU Gift city may also be encouraged to undergo the said certification course.**

2.4.4 REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA (FIU-IND)

In terms of Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and in terms of Rule 7 thereof, the reports as mentioned in Operational Guidelines Part-II, shall be furnished by the Branch to Financial Intelligence Unit- India (FIU- IND) as per guidelines prescribed by IFSCA /FIU as applicable and within the timelines specified.

Detailed guidelines regarding reporting requirements to FIU- IND have been given in Part- II Operational Guidelines of this policy.

2.4.4.1 Implementation of red flag indicators (RFIs) at branch: RFIs as prescribed by FIU shall be implemented and the same need be monitored and closed at branch level. Thresholds for implementation of RFIs shall be identified and recommended by Branch Compliance Committee to the

Governing Body for approval.

2.4.5 OTHER ASPECTS

Other KYC/AML Guidelines to be followed, e.g., Identification of Beneficial Owners, Periodic updation, Transaction monitoring, etc., are given in Part-II Operational Guidelines of the Policy such as:

- (i) Customer Due Diligence Procedure
- (ii) Identification of Beneficial Owners
- (iii) Enhanced and Simplified Customer Due Diligence
- (iv) Ongoing Due Diligence
- (v) Third Party Reliance
- (vi) Correspondent Banking and Wire Transfer
- (vii) Process of Identification of Suspicious Transactions
- (viii) Internal Policies, Compliance, Audit and Training
- (ix) Record Keeping
- (x) Other Instructions

2.5 AUTHORITY FOR APPROVING OPERATIONAL GUIDELINES

Audit Committee of Executives will be the authority for approval/ amendment of operational guidelines related to AML-CFT and KYC Policy of PNB BO: Gift City, Gujarat.

2.6 DISCLOSURE OF THE POLICY

This Policy is meant only for internal use of staff.

2.7 OWNERSHIP OF THE POLICY

Data Privacy and 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:

- (i) 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
- (ii) 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 Policy shall be approved by the Board.

(Part-II Operational Guidelines)

Operational Guidelines of Policy for Anti Money Laundering (AML)- Combating the Financing of Terrorism (CFT) and Know Your Customer (KYC) Policy of PNB IFSCA Banking Unit (IBU), GIFT City, Gujarat

(As per IFSCA Guidelines dated 17.11.2025 and Circulars issued up to 05.01.2026)

Office : IBU GIFT City
Division : Data Privacy & Management Division
Version : 2026_AML (GIFT City) _1.0



Guidelines Custodian

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

Guidelines Version Control

S. No.	Version Number	Version Date	Summary of changes
1	2021_IBD_1.0	27.01.22	New Policy
2	2023_AML (GIFT City) _1.0	06.06.23	Present Policy is prepared as per New IFSCA KYC guidelines dated 28.10.2022
3	2024_AML (GIFT City) _1.0	29.05.24	Identification of Beneficial Owner for Partnership Firm. Principal Officer, Identifying and verifying beneficiary of life Insurance Policy, Enhanced Due Diligence, Wire Transfers, CBWTR, Responsibility of The intermediary institution, Record Keeping, Reporting of Suspicious Transactions, Confidentiality of Suspicious Transaction Report, Freezing of Assets under section 51a Unlawful Activities, Obligation under Weapons of Mass Destruction (WMD), Illustrative list of documents,
4.	2025_AML (GIFT City) _1.0	30.04.25	Present Policy is prepared as per New IFSCA AML-CFT and KYC guidelines dated 10.03.25.
5	2026_AML (GIFT City) _1.0		Present Policy is prepared as per New IFSCA AML-CFT and KYC guidelines dated 17.11.2025 and Circulars issued up to 05.01.2026.

Guidelines Governance

Frequency of Review	Annual
Last reviewed on	30.04.2025
Approval Path	ACE> ACB > Board
Supersedes	2025_AML (Gift City)1.0

Operational Guidelines for AML-CFT & KYC Policy of PNB BO:IBU, GIFT City, Gujarat

This document (Part -II) Operational Guidelines is an integral part of the AML-CFT & KYC policy of PNB BO: IBU, GIFT City, Gujarat and shall be read in conjunction with the policy (Part -I).

1. DEFINITIONS

In terms of IFSCA Guidelines on AML- CFT and KYC, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

- 1.1** "Act" and "Rules" means the Prevention of Money-laundering Act, 2002 and the Prevention of Money- laundering (Maintenance of Records) Rules, 2005, respectively.
- 1.2** "Authority" or "IFSCA" means the International Financial Services Centres Authority established under sub-section (1) of section 4 of International Financial Services Centres Authority Act, 2019 (50 of 2019).
- 1.3** "Beneficial Owner" means: -
- (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 a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-

- (i) "Controlling ownership interest" means ownership of or entitlement to more than ten percent 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 ten percent of capital or profits of the partnership or who exercises control through other means;

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

- (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 or entitlement to more than fifteen percent of the property or capital or profits of the unincorporated association or body of individuals;

Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (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 ten percent 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.

Explanation: - For the purpose of determination of beneficial owner, any amendment made under sub-rule 3 of rule 9 of Rules, shall be applicable in addition to the requirements under these Guidelines.

- 1.4** “Beneficiary Institution” means the financial institution that receives the wire transfer from the ordering institution, directly or through an intermediary institution, and makes the funds available to the wire transfer beneficiary.
- 1.5** “Business Facilitator” means a person authorised by the Branch, to verify the information/officially valid documents provided by the customer for opening account with it.
- 1.6** “Central KYC Records Registry” means an entity defined under rule 2 (1) (ac) of the Rules, which is authorised to receive, store, safeguard and retrieve the KYC records of a customer in digital form.
- 1.7** “Certified Copy” means comparing the original officially valid document provided by the customer with the copy thereof and recording the same as ‘true copy’ by the authorised officer of the Branch.

Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by:

- (i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;
 - (ii) Notary Public (outside India);
 - (iii) Court Magistrate (outside India);
 - (iv) Judge (outside India);
 - (v) Certified public or professional accountant (outside India);
 - (vi) Lawyer (outside India);
 - (vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or
 - (viii) Any other authority as may be specified by the Authority.
- 1.8** “Common Reporting Standards” 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.
- 1.9** “Cover payment” means a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction (the cover) from the ordering institution to the beneficiary institution through one or more intermediary institutions.
- 1.10** “Cross-border wire transfer” means any wire transfer (including a chain of wire transfers) where either the ordering institution or the beneficiary institution is located in IFSC.

-
- 1.11** “Customer” or “Client” for the purpose of these Guidelines shall mean a person who is engaged in a financial transaction or activity with a Branch and includes a person on whose behalf the person engaged in the transaction or activity, is acting.
- 1.12** “Designated Director” means a person designated by the Bank to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules and these Guidelines.
- 1.13** “Digital KYC” means capturing the 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 Branch as per the provisions contained in the Act.
- 1.14** “Digital Signature” shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- 1.15** “Domestic Wire Transfer” means a wire transfer where both the ordering institution and beneficiary institution are located in the IFSC and also refers to any chain of wire transfers that takes place entirely within the IFSC.
- 1.16** “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 or its equivalent in other jurisdictions, as may be recognised by the Authority.
- 1.17** “FATCA” means Foreign Account Tax Compliance Act, 2010 of the United States of America (USA) which, inter-alia, requires reporting 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.
- 1.18** “Financial Group” means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
- 1.19** “Financial Intelligence Unit – India” refers to a national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions.
- 1.20** “Governing Body” means, a committee constituted as per Governance Framework Policy for PNB, B.O. IBU GIFT City, Gujarat approved by the Board.
- 1.21** “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).
- 1.22** “International Financial Services Centre” shall have the meaning assigned to it under clause (g) of sub- section (1) of Section 3 of the IFSCA Act, 2019 (50 of 2019).
- 1.23** “Intermediary Institution” means the financial institution in a serial payment or

cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.

1.24 “International Organisation PEP” means a person who is or has been entrusted with prominent function by an international organisation.

Explanation: This may include members of Senior Management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors and members of the board or equivalent functionaries. An international organisation includes any organisation set up either by the governments of more than one country or by international organisation(s).

1.25 “Know Your Client (KYC) Identifier” means the unique number or code assigned to a customer by the Central Know Your Customer Records Registry.

1.25A. “KYC Registration Agency (KRA)” means an entity which has been granted certificate of registration under the International Financial Services Centres Authority (KYC Registration Agency) Regulations, 2025.

1.26 “Money Laundering” shall have the meaning assigned to it under section 3 of the Act and “Anti-Money Laundering” shall be construed accordingly, and shall include Counter-Terrorist Financing and other related measures.

1.27 “Non-face-to-face customers” means customers who open accounts without visiting the Branch or meeting the authorized officials/persons of the Branch.

1.28 “Non-profit organisation” means any entity or organisation, 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 (21 of 1860) or any similar State legislation or a company registered under section 8 of the Companies Act, 2013 (18 of 2013) or other legal entity from any other jurisdictions, which is engaged in not-for-profit activities, and is recognised as such by the Authority.

Explanation: Every Regulated Entity in the form of Banking Unit, Financial Institution or Intermediary, as the case may be, shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of 11[five years] after the business relationship between a client and the aforementioned entity has ended or the account has been closed, whichever is later.

For avoidance of doubts, it is clarified that, the definition of ‘Financial Institution’ and ‘Intermediary’ shall have the meaning as defined under the section 2(1)(l) and 2(1)(n) respectively, of the Act.

1.29 “Non- Resident Indian” shall have the meaning as defined in Foreign Exchange Management (Deposit) Regulations, 2016.

1.30 “Ordering Institution” means the financial institution that initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer

on behalf of the wire transfer originator.

- 1.31** “Officially Valid Document” means the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card issued by the Election Commission of India or letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator;

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

Provided further that, where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be ‘officially valid document’: -

- a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- b) Letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided also that,

where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document **or the equivalent e-documents thereof** shall also be deemed to be Officially Valid Document:

- 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, Municipal tax receipt, or such other equivalent document;**
- iii. Post Office savings bank account statement or statement of a bank account including of a foreign bank;
- iv. pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- v. 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; and

Provided also that in case the Officially Valid Document 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;

Provided also that where the client submits his proof of possession of AADHAAR number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.

Explanation: For the purpose of this Clause, a document shall be deemed to be an Officially Valid Document 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.

1.32 “Person” means and includes:

- a) an individual;
- b) a Hindu undivided family;
- c) a company;
- d) a partnership firm;
- e) a limited liability partnership;
- f) an association of persons or a body of individuals, whether incorporated or not;
- g) every artificial juridical person not falling within any of the above; and
- h) any agency, office or branch owned or controlled by any of the above.

1.33 “Periodic Updation” means steps taken to ensure that documents, data or information collected under the Customer Due Diligence process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity specified by the Authority.

1.34 “Principal Officer” means an officer designated by the Bank as such, who shall be responsible for furnishing information as required under rule 8 of the Rules. Provided that such officer shall be an officer at the management level.

1.35 “Politically Exposed Person” means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

Explanation: The definition of Politically Exposed Person is not intended to cover middle ranking or more junior individuals in the definition.

1.36 “Regulated Entity” means IFSC Banking Unit (IBU) of Punjab National Bank at GIFT City, Gujarat, which has been granted license by IFSCA.

1.37 “Senior Management” means management as defined in Governance Framework Policy for PNB, B.O. IBU GIFT City, Gujarat approved by the Board.

1.38 “Serial Payment” means a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the

ordering institution to the beneficiary institution, directly or through one or more intermediary institutions.

- 1.39** “Shell financial institution” means a bank or financial institution incorporated, formed or established in a country or jurisdiction where the bank or financial institution has no physical presence, and which is unaffiliated with a financial group that is subject to effective supervision.

“Explanation: Physical presence means meaningful mind in the form of senior management located within an IFSC. The existence simply of a local agent or low-level staff does not constitute physical presence.”

- 1.40** “Straight-through processing” means payment transactions that are conducted electronically without the need for manual intervention.

- 1.41** “Suspicious Transaction” means a “Transaction” as defined in these Guidelines, including an attempted transaction, which to a person acting in good faith-

- a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to have no economic rationale or bona-fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

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

- 1.42** “Transaction” means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

- a) opening of an account;
- b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether by 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; and
- f) establishing or creating a legal person or legal arrangement.

- 1.43** “Unique transaction reference number” means 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, which permits the traceability of the wire transfer.

1.44 “Video based Customer Identification Process” or “V-CIP” means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the Branch **or financial group entity in India supervised by a financial regulator or a KRA Registration Agency**, by undertaking seamless, secure, live, informed & consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

Explanation: - Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification procedure for the purpose of these Guidelines.

1.45 “Wire Transfer” means any transaction carried out on behalf of a Wire Transfer Originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a Beneficiary Institution, irrespective of whether the originator and the beneficiary are the same person.

1.46 “Wire Transfer Beneficiary” means the natural person, legal person or legal arrangement who is identified by the wire transfer originator as the receiver of the wire transfer funds.

1.47 “Wire Transfer Originator” means the account holder who allows the wire transfer from that account; or where there is no account, the natural person, legal person or legal arrangement that places the wire transfer order with the ordering institution to perform the wire transfer.

Note: - Words and expressions used but not defined in these Guidelines shall have the same meaning as assigned to them under the International Financial Services Centres Authority Act, 2019, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

2. RISK BASED APPROACH

- a)** The primary thrust of these Guidelines is to enable the Branch to adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which the Branch is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same. The Branch while adopting RBA shall ensure that:
- (i) The RBA is objective and proportionate to the risks;
 - (ii) The RBA is based on reasonable grounds; and
 - (iii) The RBA is reviewed and updated at appropriate intervals.

- b) The RBA shall be appropriate to the nature and size of the business. While implementing the RBA, the Branch shall consider all relevant risk factors before deciding overall risk. Based on the risk assessment, the Branch shall monitor, manage, and mitigate the risks it is exposed to by applying effective, appropriate and proportionate measures.
- c) In addition to assessing the ML/TF risks presented by an individual customer, the Branch shall also identify and assess ML/TF risks at an enterprise-wide level (Financial Group-wide level or Group-wide level) wherever applicable. This shall include a consolidated assessment of the Branch's ML/TF risks perception that exist across all its business units, product lines and delivery channels.

Explanation: FATF Public Statement, the reports and guidance notes on AML/CFT/PF issued by FATF and any country specific information that is circulated by relevant authorities from time to time, as well as the updated list of natural and legal persons who are subjected to sanction measures as required under various United Nations' Security Council Resolutions, etc., may also be used in risk assessment.

- d) The outcome of the risk assessment by the Branch shall be properly documented. The documentation should include the enterprise-wide AML/CFT risk assessment wherever applicable, details of the implementation of the AML/CFT risk management systems and controls as guided by the AML/CFT risk assessment. The Branch shall ensure that the ML/TF risk assessment information are made available to the Authority upon request. The records of documented risk assessment shall be kept as per the requirements of record keeping process specified under these Guidelines.
- e) The result of the risk assessment shall be used to classify the ML/TF risks as low, medium, and high. The general principle of this classification is to apply enhanced measures in case of high-risk customers and simplified measures in case of low-risk customers.
- f) To keep the risk assessments up-to-date, the Branch shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Governing Body.

Guidance Note: -

The RBA should be an essential foundation in Branch's AML-CFT compliance culture, and it must trickle down from the level of Senior Management to the rest of the organization.

3 BUSINESS RISK ASSESSMENT

3.1. Identifying and Assessing business AML risks

The Branch shall:

- (a) take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to ML/TF risks;
- (b) consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the ML/TF risks: -
 - (i) its type of customers and their activities;
 - (ii) its business engagement with the countries or geographic areas;
 - (iii) its products, services, delivery channels and activity profiles;
 - (iv) the complexity and volume of its transactions;
 - (v) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
 - (vi) the use of new or developing technologies for both new and pre-existing products;
- (c) based on the assessment and risk identification made at Clause (a) and (b) above, the Branch shall undertake commensurate mitigation measures.

3.2. New products, business practices and technologies

- (a) The Branch shall identify and assess the ML and TF risks that may arise in relation to: -
 - (i) the development of new products, business practices, including new delivery mechanisms; and
 - (ii) the use of new or developing technologies for both new and pre-existing products.
- (b) The Branch shall undertake the above risk assessment exercise, prior to the launch or use of such products, practices and technologies and shall take appropriate measures to manage and mitigate the risks.

Guidance Note: -

1. One of the key reasons for undertaking the exercise of business risk assessment is that it will aid the Branch to better understand its exposure to ML/TF risks and then take appropriate measures to prevent its business being used for the purposes of ML/TF. The risk exposure of the Branch varies depending on several factors such as the nature of the business, the type of customers, the nature of the products, services offered, and transactions and delivery channels involved.
2. The outcome of the business risk assessment should be used by the Branch to gauge its own vulnerabilities to ML/TF risks and to take all

necessary measures to mitigate such risks.

3. The outcome of the business risk assessment shall be factored into while assessing the customer risk assessment, in the manner as specified under Clause 4.

3.3. AML/CFT systems and controls

- (a) The nature and extent of AML/CFT systems and controls implemented by the Branch shall be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, wherever applicable. The Branch shall put in place adequate policies, procedures, systems and controls to mitigate such ML/TF risks. The information obtained from the risk assessment shall be used to:
 - (i) establish and maintain effective policies, procedures, systems and controls to prevent ML/TF;
 - (ii) ensure that the Branch's AML/CFT policies, procedures, systems and controls adequately mitigate the risks identified under Clause 3.1 above;
 - (iii) ensure that Branch's systems and controls:
 - (aa) include a provision enabling its Senior Management to regularly review the information on operations and effectiveness of its AML systems and controls;
 - (bb) enable the Branch to determine:
 - (1) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP); and
 - (2) whether a beneficiary of the policy, or a Beneficial Owner of such beneficiary is a PEP, (in the cases where it is providing life insurance or other similar policies); and
 - (3) enable the Branch to comply with these Guidelines and applicable AML-CFT legislations.
 - (iv) ensure that regular risk assessments are carried out on the adequacy of the Branch's AML/CFT systems and controls to enable it to identify, assess, monitor, manage and mitigate such risks adequately.
- (b) The AML/CFT policies, procedures and controls shall be approved by Senior Management to enable the Branch to effectively manage and mitigate the risks either identified by it or notified to it by the Authority or other relevant authorities. Further, the Branch shall constantly monitor the implementation of the policies, procedures and controls, and improve them, if necessary.

Guidance Note

- (1) The Branch's ML/TF risk assessment serves as a guide to the allocation of AML/CFT resources within it.

- (2) In the context of Clause (a)(iii)(bb)(2) above, beneficiary may be a natural person, legal person, legal arrangement, or category of persons who will be paid the policy proceeds when an insured event occurs, that is covered by the policy.

4 CUSTOMER RISK ASSESSMENT

Risks identified while assessing the business risks shall be used for the customer risk assessment. The customer risk assessment shall be performed while taking into consideration the parameters, or the process as specified below. The outcome of the Customer risk assessment shall be used to assign the risk rating of the customer as high, medium or low, proportionate to the ML/TF risks.

4.1 Assessing customer AML risks

- (a) The Branch shall:
- (i) undertake a risk-based assessment of every customer; and
 - (ii) assign the customer a risk rating proportionate to the ML/TF risks.
- (b) The customer risk assessment referred to in Clause (a) above, shall be completed prior to undertaking Customer Due Diligence for new customers, and also where the Branch otherwise feels necessary, for existing customers.
- (c) When undertaking an assessment under Clause 4.1(a)(i) above, the Branch shall:
- (i) identify the customer and Beneficial Owner, if any;
 - (ii) obtain information on the purpose and intended nature of the business relationship;
 - (iii) obtain information on, and take into consideration, the nature of the customer's business;
 - (iv) take into consideration the nature of the customer, its ownership, control structure, and its Beneficial Ownership, wherever applicable;
 - (v) take into consideration the nature of the customer's business relationship with the Branch;
 - (vi) take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;
 - (vii) take into consideration the relevant product, service or transaction; and,
 - (viii) take into consideration the beneficiary of the policy including any Beneficial Owner of such beneficiary, if it is providing the customer with a life insurance or other similar policy.
- (d) **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.**

4.2 Factors that may indicate high ML/TF risk

When assessing if there is a high risk of ML/TF in a particular situation, the Branch shall take into account, among other things:

(a) Customer risk

- (i) Whether the customers are from high-risk businesses / activities / sectors, as well as from other sectors as may be identified by it;
- (ii) Whether the ownership structure of the legal person or arrangement appears unusual or excessively complex;
- (iii) Whether the business relations are conducted under unusual circumstances (e.g., significant unexplained geographic distance between the Branch and the customer);
- (iv) Whether the companies have nominee shareholders or shares in bearer form;
- (v) Whether the legal persons or legal arrangements are personal asset holding vehicles; and,
- (vi) Whether the corporate structure of the customer is unusual or excessively complex given the nature of the business.

(b) Country or Geographic risk

- (i) Whether the countries or jurisdictions the Branch is exposed to, either through its own activities or the activities of its customers (including the Branch's network of correspondent account relationships) have relatively high levels of corruption, organized crime or inadequate AML/CFT measures, as identified by the FATF;
- (ii) Whether the countries or jurisdictions are identified by any credible body as having significant levels of corruption, terrorism financing or other criminal activities;
- (iii) Whether the countries or jurisdictions are identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;
- (iv) Whether the countries or jurisdictions do not have effective systems to counter ML/TF; or not implementing the AML/CFT measures that are consistent with FATF Recommendations;
- (v) Whether the countries or jurisdictions are subject to sanctions, embargos or similar measures issued by International Organisations or India;
- (vi) Whether the countries or jurisdictions are funding or supporting the terrorism; and,
- (vii) Whether countries or jurisdictions have organizations operating within their territory that have been designated by India, other countries or International Organizations as terrorist organizations.

(c) Product, Service, Transaction or Delivery Channel risk factors

- (i) Whether the service involves private banking;
- (ii) Whether the product, service or transaction is one that might favour anonymity;
- (iii) Whether the situation involves non-face-to-face business relationships or transactions, without adequate safeguards;
- (iv) Whether the payments received are from unknown or unassociated third parties;
- (v) Whether the services offered are in relation to nominee directors, nominee shareholders or the formation of companies in another country; and
- (vi) Whether there are anonymous transactions or any transaction which involves frequent payments, received from unknown or unassociated third parties.

While assessing the risk factors, the Branch shall examine the overall risk, keeping in mind that the presence of one or more risk factors alone may not always indicate a high risk of ML/TF in a particular situation.

4.3 Factors that may indicate low ML/TF risks

When assessing if there is a low risk of ML/TF in a particular situation, the Branch shall take into account, among other things:

(a) customer risk factors, including whether the customer is:

- (i) a Government entity;
- (ii) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- (iii) regulated financial institution incorporated or established outside India that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.
- (iv) a subsidiary of a regulated financial institution referred to in sub-clause (iii) above, if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML standards as that of its Parent entity;
- (v) a public body or a publicly owned enterprise;
- (vi) a resident established or registered in a geographical area of low risk;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

- (i) a Contract of Insurance that is non-life insurance;
- (ii) a Contract of Insurance that is a life insurance product with no investment

- return or redemption or surrender value;
- (iii) an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;
 - (iv) a Contract of Insurance which is a reinsurance contract that is ceded by an insurer which is a regulated financial institution;
 - (v) a pension, superannuation or similar scheme that satisfies the following conditions:
 - (aa) the scheme provides retirement benefits to employees;
 - (bb) contributions to the scheme are made by way of deductions from wages; and
 - (cc) the scheme rules do not permit the assignment of a member's interest.
 - (vi) a product where the ML/TF risks are adequately managed by other factors such as transaction limits or transparency of ownership; and
 - (vii) financial products or services that provide appropriately defined and limited services to certain types of customers (e.g., to increase customer access for financial inclusion purposes).

When assessing the risk factors, the Branch shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a low risk of ML/TF in a particular situation.

4.4 Business relationship should not be established in the following cases:

The Branch shall not establish the business relationship with the customer, which is a legal person or legal arrangement, in the following cases: -

- (a) where the ownership or control arrangements of the customer prevent the Branch from identifying one or more of the customer's Beneficial Owners;
- (b) where there are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the Branch or a Shell Financial Institution.

Guidance Note for Customer Risk Assessment

- (1) The risk assessment requires the Branch to allocate an appropriate risk rating to every customer. **Before undertaking Customer Due Diligence on a new customer, IBU needs to undertake a customer risk assessment and assigns the customer a risk rating proportionate to the customer's money laundering risks, using the Customer Risk Assessment template attached in Annexure – IV.** The risk ratings should be descriptive, such as “low”, “medium” or “high”. The outcome of the ML/TF risk assessment decides the degree of Customer Due Diligence that need to be performed. For a high-risk

customer, the Branch shall undertake Enhanced CDD measures in addition to the normal CDD. For a low-risk customer, the Branch may undertake Simplified CDD. For any other customer, the Branch may undertake the normal CDD.

- (2) Where information obtained as part of CDD alters the risk rating of a customer, such change should reflect in its CDD being undertaken.

5 CUSTOMER DUE DILIGENCE

5.1. Customer Due Diligence Process: The Branch after assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the Customer Due Diligence. While undertaking the CDD, the Branch shall: -

- (i) undertake Customer Due Diligence measures as detailed under Clause 5.4, in respect of all the customers;
- (ii) undertake Enhanced Customer Due Diligence measures as detailed under Clause 5.6, in addition to the CDD measures detailed under Clause 5.4, in respect of the customer who has been assigned ‘high risk’; and,
- (iii) undertake Simplified Customer Due Diligence measures as detailed under Clause 5.7 by modifying Customer Due Diligence process detailed under Clause 5.4, in respect of a customer who has been assigned ‘low risk’.

5.2. Timing of CDD

- (a) Except as otherwise provided in Clause 5.3 and 5.4, the Branch shall undertake the Customer Due Diligence of a customer: -
- (i) at the time of establishing business relationship, as mandated under Clause 5.4.1 (a) to (c); and,
 - (ii) after establishing a business relationship, as mandated under Clause 5.4.1. (d).
- (b) The Branch shall also undertake Customer Due Diligence if, at any time:
- (i) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;
 - (ii) it suspects ML/TF; or,
 - (iii) there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

5.3. Establishing business relationship before verification

- (a) The Branch may establish a business relationship with a customer before completing the verification required under Clause 5.4.1, subject to fulfilling the following conditions:

- (i) the deferral of completion of the verification of the customer or Beneficial Owner is essential in order not to interrupt the normal conduct of a business relationship;
 - (ii) there is low risk of occurrence of ML/TF activity and any such risks identified can be effectively managed by the Branch;
 - (iii) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed, and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and
 - (iv) subject to Clause 5.3(b) below, the relevant verification is completed as soon as reasonably practicable and, in any event, it should not exceed 30 business days after the establishment of business relationship.
- (b)** Where the Branch is not able to comply with the 30-day requirement, it shall, prior to the end of the 30-day period:
- (i) document the reason for its non-compliance;
 - (ii) complete the verification as soon as possible; and
 - (iii) record the non-compliance event for reporting to its Governing Body.
- (c)** The Branch shall suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that is possible) if such verification remains uncompleted for 30 days after the establishment of business relationship.
- (d)** The Branch shall terminate business relations with the customer if such verification remains uncompleted for 120 days after the establishment of business relationship.
- (e)** The Branch shall ensure that its AML/CFT systems and controls referred to in Clause 3.3 above, include internal risk management policies and procedures concerning the conditions under which such business relationships may be established with a customer before completing verification and should also factor the above time limitation in its policies, procedures and controls.

Guidance Note: -

- (1) Examples of the situations which might lead the Branch to have doubts about the veracity or adequacy of documents, data or information previously obtained, could be where there is a suspicion of ML/TF in relation to that customer, or where there is a material change in the manner the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Branch that a person other than the customer is the real customer.
- (2) Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business,

may include:

- a) Non-face-to-face business.
- b) Securities transactions. In the securities market, companies and intermediaries may be required to perform transactions without delay depending upon market conditions, and in such circumstances, the execution of the transaction may be required before verification of identity is completed. Similar circumstances may occur where the customer seeks immediate insurance cover.
- (3) In case the Branch is not able to complete customer due diligence as required under Clause 5.4, it shall not commence or continue business relations with any customer or undertake any transaction for any customer. In case of failure to complete customer due diligence in the prescribed time limit, the Branch shall apply appropriate measures as specified under Clause 5.10. The Branch shall also consider filing of STR if the circumstances are suspicious.
- (4) The Branch shall also adopt risk management procedures in the cases specified under Clause 5.3. These procedures shall include a set of measures, such as a limitation of the number, types and/or value of transactions that can be performed. The procedures shall also include the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. In such situations, the Branch shall ensure close monitoring, until the verification is completed.

5.4. Customer Due Diligence Requirements

5.4.1. Undertaking Customer Due Diligence (CDD)

In undertaking Customer Due Diligence as required under Clause 5.1.(a)(i), the following measures shall be undertaken by the Branch: -

- (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- (b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that the Branch is satisfied that it knows who the beneficial owner is. Similarly, for legal persons and arrangements, the CDD shall include Branch taking reasonable steps to understand the nature of the customer's business, its ownership and control structure.
- (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Branch's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

5.4.2. Identification of Customer

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

- (a) If a customer is a natural person, the Branch shall obtain at least the following information:
- (i) Full name, including any aliases;
 - (ii) Unique Identification Number (such as an Identity card number, passport number, etc.);
 - (iii) Date of birth;
 - (iv) Nationality;
 - (v) Legal domicile;
 - (vi) Current residential address; (other than a post office box address);
 - (vii) Contact details such as personal, office or work telephone numbers.
- (b) If a customer is a legal person or legal arrangement, the Branch shall obtain at least the following information:
- (i) The full name and any trading name;
 - (ii) Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);
 - (iii) Registered or business address, and if different, its principal place of business;
 - (iv) Date of establishment, incorporation or registration;
 - (v) Place of incorporation or registration.
- (c) Further, in cases where the customer is a legal person or legal arrangement, the Branch shall, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. In addition to this, Branch shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, the Branch shall obtain at least the following information of each related or connected party:
- (i) full name, including any aliases; and
 - (ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

Guidance Note: -

- 1) The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties, or which is his place of origin.
- 2) The Branch should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required under Clause 5.4.2.(a), the Branch should (if not already obtained as part of its account opening process) also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income, other related accounts with the same Branch and whether the customer holds or has held a prominent public position. Such additional identification information enables the Branch to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account.
- 3) Identification of connected parties or related parties may be undertaken

using publicly available sources or databases such as company registries, annual reports. Additionally, it could be based on substantiated information provided by the customers.

5.4.3. Verification of Identity of Customer

- (a) The Branch shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, the Branch shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.
- (b) When relying on documents, the Branch should be aware that the most reliable documents to verify the identity of the customer are those which are most difficult to obtain illegally or to counterfeit. These may include government-issued identity cards or current valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process should be commensurate with the customer's risk profile.
- (c) In verifying the identity of a customer, the Branch may obtain the following documents:

In case of Natural Persons –

- (i) any of the OVD specified under these Guidelines that contains photograph of the customer, name, unique identification number, date of birth and nationality; and
- (ii) residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

In case of Legal persons or Legal Arrangements-

- (i) **Name, legal form, proof of existence and constitution:** - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and
- (ii) **Powers that regulate and bind the legal person or legal arrangement:** - This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories.

Guidance Note: -

- (1) In cases where a customer is a natural person, the Branch shall obtain the OVD that contain a clear photograph of that customer.
- (2) In cases where a customer is a foreign national, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national would also be considered

as OVD. In case where the customer is an Indian national, OVD shall include the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card, etc. as prescribed under the Rules (For more detailed understanding, refer OVD definition). For the purpose of customer verification, equivalent e-documents of OVDs shall also be treated as original document by the Branch.

- (3) Where a customer submits any documents other than Post Office savings bank account statement or statement of a bank account including of a foreign bank, as specified at the third proviso of clause 1.3.30 for limited purpose of proof of address, such customer shall submit updated OVD or their equivalent e-documents thereof with current address within a period of three months of submitting the documents specified at the third proviso of clause 1.3.30 above.**

Explanation: - The bank account or Post Office savings bank account statement or statement of foreign bank may be accepted as deemed OVD for the limited purpose of proof of address, only for such customers where simplified measures are applied."

- (4) While undertaking CDD for different customers (including legal persons or legal arrangements), the Branch should obtain such information and documents as required under these Guidelines. Illustrative list of information and documents which should be obtained for on boarding customers are specified in ***Annexure-I*** of these Guidelines.
- (5) Further, for on boarding Indian Nationals, the Branch may follow the procedure as specified under ***Annexure-II*** of these Guidelines.
- (6) The Branch should examine the original identification documents and retain a copy of the same. However, in complying with Clause 5.4.1, (i.e., undertaking customer due diligence), at times, if a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where the Branch has no physical contact with the customer or the on boarding of customer is done through non-face to face mode), the Branch should obtain a copy of the document that is certified to be a 'true copy' and such certification may be carried out by person specified in Clause 1.7 of these Guidelines.
- (7) The Branch shall ensure that documents obtained for performing CDD, as required under these Guidelines, are clear and legible. This is important for the establishment of a customer's identity, particularly in situations where business relations are established through non-face to face mode.
- (8) Except for high-risk customers, the following mode of verifications are also considered as sufficient to satisfy the requirements of Clause 5.4.3: -
- (i) downloading publicly available information from an official source (such as a regulator's or other official government website);
 - (ii) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information

found on the internet and commercial databases, provided that the commercial database is recognized for such purpose by the home regulator, if any, of the database.

- (9) Where the Branch obtains data, documents or information from the customer or a third party, it shall ensure that such data, documents or information is up-to-date.
- (10) Where the customer is rated as high-risk, the identification information shall be independently verified, using both public and non-public sources.

5.4.4. Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer

- (a) Where a customer is a natural person or legal person **or legal arrangement** and appoints one or more natural persons to act on its behalf for establishing business relations with the Branch, the Branch shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person **or legal arrangement** by obtaining information as specified in Clause 5.4.2 above.

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 following transactions: -

- 1. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.**
- 2. 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.**
- 3. 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.**

- (b) Further, the Branch shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, the Branch shall verify the authorisation of each natural person appointed to act on behalf of the customer by obtaining at least the following:-

- (i) The appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf which may include power of attorney, resolution passed by Governing Body or authorisation granted to transact on its behalf.
- (ii) Where there is a long list of natural persons appointed to act on behalf of the customer (e.g., a list comprising more than 10 authorized signatories), the Branch shall verify those natural persons who will deal directly with the Branch.

5.4.5. Identification and Verification of Identity of Beneficial Owners

Where there is one or more Beneficial Owners in relation to a customer, the Branch

shall identify the Beneficial Owners and take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources. For the identification and verification of Identity of Beneficial Owner, the Branch should consider the following in relation to:-

(a) Customers that are legal persons

- (i) The identity of the natural person(s) (whether acting alone or together) exercising control over the legal person through ownership or who ultimately owns the legal person;
- (ii) To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural person(s) (if any) who ultimately control the legal person or have ultimate effective control over the legal person.

(b) Customers that are legal arrangements

- (i) 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 ten per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- (ii) In all other types of legal arrangements, the Branch shall identify persons in equivalent or similar positions.

5.4.6. Parameters to Identify and Verify the Identity of Beneficial Owners: -

- (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 or entitlement to more than ten percent 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 ten per cent of capital or profits of the partnership;
- (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 or entitlement to more than fifteen per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: The term ‘body of individuals’ includes societies. Where no natural person is identified under (a) to (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 ten per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

5.4.7. As per rule 9(3)(f) of the Rules, unless the Branch has doubts about the veracity of the CDD information, or suspects that customer may be connected with ML/TF, it shall not be required to identify and verify the identity of any shareholder or beneficial owner of a customer in the following –

Where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a customer under the Act and Rules.

5.4.8. As per the second proviso of rule 9(1)(c) of the Rules, in cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in sub-rules (3) to (9) of the rule 9 of the Rules shall be applicable for due- diligence of such beneficial owner.

Guidance Note: -

- (1) For opening an account of a Legal Person who is not a natural person, the Branch has to identify the beneficial owner(s) and shall undertake all reasonable steps to verify his/her identity in terms of sub- rule (3) of rule 9 of the Rules.
- (2) The Branch may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.
- (3) Notwithstanding the obtaining of such an undertaking or declaration, the Branch remains responsible for complying with the obligations under the Guidelines to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by

the customer.

- (4) Where the customer is not a natural person and has a complex ownership or control structure, the Branch should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.
- (5) Where the Branch has exhausted all possible means but has not been able to identify the Beneficial Owners under Clause 5.4.5., it shall treat the Senior Management of the said legal person or legal arrangement, as the Beneficial Owners. However, in such cases, the Branch shall keep a record of all the actions it has taken to identify the Beneficial Owners of such legal persons or legal arrangement.
- (6) If the ownership or control arrangements of a customer are of such a nature that the Branch is prevented from identifying the Beneficial Owners, the Branch shall not establish a business relationship with the customer under Clause (a) of 4.4.
- (7) In relation to Clause 5.4.7 and Clause 5.4.8 above, currently the notified jurisdictions by Central Government are as follows: -
 - (a) United States of America
 - (b) Japan
 - (c) South Korea
 - (d) United Kingdom excluding British Overseas Territories
 - (e) France
 - (f) Germany
 - (g) Canada
- (8) Where the customer is not a natural person, the Branch shall understand the nature of the customer's business, its ownership and control structure, before opening an account.

5.4.9. Identifying and verifying beneficiary of a life insurance policy

For life or other investment-related insurance business, the Branch shall, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

- (i) The Branch shall, as soon as a beneficiary of a life policy is identified as a specifically named natural person, legal person or legal arrangement, obtain the full name, including any aliases, of such beneficiary;
- (ii) For beneficiary(ies) that are designated by characteristics or by class (e.g., spouse or children at the time that the insured event occurs) or by other means (e.g., under a will) – the Branch shall obtain sufficient information concerning the beneficiary(ies) to satisfy itself that it will be able to establish the identity of the beneficiary(ies) at the time of the payout.
- (iii) in relation to life insurance policies, the Branch should be required to take reasonable measures to determine whether the beneficiaries and/or, where

required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, it will be required to inform Senior Management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a Suspicious Transaction Report.

Guidance Note: -

- (1) For both the cases referred to in (i) and (ii) of the Clause 5.4.9 above, the verification of the identity of the beneficiary(ies) should be conducted at the time of the payout.
- (2) The information collected under (i) and (ii) of the Clause 5.4.9 above, should be recorded and maintained in accordance with the record keeping requirements under these Guidelines.
- (3) The beneficiary of a life insurance policy should be included as a relevant risk factor by the Regulated Entity in determining whether enhanced CDD measures are applicable. If the Branch determines that a beneficiary who is a legal person or a legal arrangement presents a high risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

5.4.10. Information on the Purpose and Intended Nature of Business Relations

- (a) The Branch shall, while establishing business relationship, understand and as appropriate, obtain information from the customer as to the purpose and intended nature of business relations.
- (b) The measures taken by the Branch to understand the purpose and intended nature of business relations should be commensurate with the risk profile and complexity of the customer's business.

5.5. Accounts of Politically Exposed Persons

- (a) The Branch shall implement appropriate internal risk management systems, policies and procedures to determine if a customer or any natural person appointed to act on behalf of the customer, or any beneficial owner of the customer is a politically exposed person (PEP) or in case of a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP.
- (b) The Branch shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer or beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary is determined by the Branch to be a PEP:
 - (i) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family

- members, any beneficial owner and close relatives;
- (ii) Verify the identity before accepting the PEP as a customer;
 - (iii) Obtain approval from its Senior Management before opening an account of a PEP or making any pay out under the life insurance or other similar policy to the PEP;
 - (iv) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;
 - (v) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.
 - (vi) Carry out the additional Customer Due Diligence for circumstances specified in sub-clauses (i) to (v) above, before making any payout under the life insurance or other similar policy.
- (c) The Branch may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for:-
- (i) PEP, their family members and close associates;
 - (ii) International Organisation PEP, their family members, and close associates; or
 - (iii) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Regulated Entity present a high risk for ML/TF.

Guidance Note: -

- (1) The Branch is required to take reasonable measures to determine whether a customer or beneficial owner is a PEP or a person who is or has been entrusted with a prominent function by an international organisation.
- (2) The Branch shall also ascertain the source of wealth of the customers by appropriate and reasonable means. (Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns, bank statements, etc.).
- (3) The Branch should be aware that customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves. Therefore, the measures applied for all types of PEPs should also apply to family members or close associates of such PEPs.
- (4) The Branch should not automatically treat all individuals who are PEPs, as a high-risk customer. Each PEP should be assessed on risk sensitive basis and the Branch shall determine what risk category is appropriate for such

PEPs. In case a PEP is assigned as high risk, the Branch shall undertake the Enhanced Customer Due Diligence measures referred under Clause 5.6. However, even if a PEP is not assigned a high risk, the Branch shall still undertake the additional customer due diligence measures specified in Clause 5.5 (b) for PEPs.

- (5) Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e., total assets). This relates to how the customer and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have. Although the Branch may not have specific information about assets that are not deposited with or processed by the Branch, it may be possible to obtain general information from the customer, commercial databases or other open sources.
- (6) Verification of source of wealth can be carried out by various measures including obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, information and documents such as evidence of title, copies of trust deeds, bank or brokerage account statements, probate documents, audited accounts and financial statements, salary details, tax returns, news items from a reputable source and other similar evidence. For instance:
 - (i) for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and
 - (ii) for a natural person, this might include documentary evidence which corroborates answers given to questions on the source of wealth in an application form or customer questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide bank statements, salary statements or tax returns covering number of years to draw up a picture of his source of wealth.

5.6. Enhanced Due Diligence

- (a) Where the risks of ML/TF are high, the Branch shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows: -
 - (i) Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
 - (ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source

- of funds of the customer or, if applicable, of the Beneficial Owner.
- (iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
 - (iv) Obtaining the approval of Senior Management to commence or continue the business relationship.
 - (v) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,
 - (vi) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
- (b) Where applicable, it is required that first payment made by a customer in order to open an account with the Branch shall be carried out through a bank account in the customer's name with:
- (i) a Bank;
 - (ii) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or
 - (iii) a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.
- (c) The Branch shall specifically apply enhanced due diligence measures, 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.

Guidance Note: -

- (1) The Enhanced CDD measures will apply depending upon the risk profile of the customer and the extent of its applicability to a customer shall be decided on case-to-case basis.
- (2) Circumstances where a customer presents or may present a high probability of ML/TF risk may include, but are not limited to the following:
 - (i) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for counter measures; and
 - (ii) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the Branch for itself or notified to the Branch generally by the Authority or other relevant domestic authorities in India or other foreign regulatory authorities.
- (3) For establishing an account-based relationship with high-risk customers, the approval may be given by Senior Management or committee of senior managers or an individual member who has been authorised by the Senior

Management in this behalf.

- (4) In cases where a customer uses complex legal structures and/or trusts, private investment vehicle, the Branch shall satisfy itself that it is used for a legitimate and genuine purpose.
- (5) The Branch shall take reasonable measures to examine the source of wealth and source of funds. That is, where the funds for a particular service or transaction will come from (e.g., a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.
- (6) Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations. In order to ensure that the funds are not proceeds of crime, the Branch should not limit its source of funds inquiry to identifying the other financial institution from which the funds have been transferred, but more importantly, the activity that generated the funds. The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired.
- (7) Examples of appropriate and reasonable means of establishing source of funds are such as proof of dividend payments connected to a shareholding, bank statements, salary payments or bonus certificates, sale proceeds, loan documentation and proof of a transaction which gave rise to the payment into the account.
- (8) A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.
- (9) **To maintain transparency and mitigate the risk of round-tripping, the Regulated Entity shall endeavor to ascertain the source of funds in cases where the Beneficial Owner of an entity is an Indian National. In such instances, the Regulated Entity shall apply the enhanced due diligence measures specified under point (ii) of sub-clause (a) of clause 5.6 above, irrespective of the risk categorization assigned to such Non-Resident customer.**

5.7. Simplified Customer Due Diligence

- (a) Where the risks of ML/TF are low, the Branch may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:
 - (i) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship as specified under Clause 5.3.
 - (ii) Reducing the frequency of customer identification updates.

- (iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- (iv) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.
- (b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.

Guidance Note: -

- (1) Where the Branch applies SCDD measures, it is still required to perform ongoing monitoring of business relations as specified under Clause 5.8.
- (2) The Branch is not required to identify or verify Beneficial Owners for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions.
- (3) The Branch may also use other measures to conduct CDD in accordance with the customer risks.

5.8. Ongoing Customer Due Diligence

While undertaking the ongoing customer due diligence, as required under Clause 5.4.1.(d), the following requirements shall be complied with by the Branch:-

- (i) The Branch shall monitor its business relations with the customer on an ongoing basis.
- (ii) The Branch during the course of business relations with a customer, shall observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with Branch's knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.
- (iii) The Branch shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.
- (iv) The Branch shall make further enquiries into the background and purpose of the transaction specified in sub-clause (iii) above and document its findings so that this information is made available to the relevant authorities, should the need arise.
- (v) The Branch shall periodically review each customer to ensure that the risk rating assigned under Clause 4.1.(a)(ii) above, is commensurate with the ML/TF risks posed by the customer.
- (vi) Where there are indications that the risks associated with an existing business relation with the customer may have increased, the Branch shall request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

- (vii) The Branch shall ensure that the Customer Due Diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Customer Due Diligence data, documents and information, particularly for customers with high-risk rating.

Guidance Note: -

- (1) For an effective and robust AML/CFT risk management system, the Branch shall follow the process of Ongoing monitoring of all business relations. However, the rigor and extent of monitoring of a customer shall be determined based on the customer's ML/TF risk profile.
- (2) An essential aspect of ongoing monitoring includes maintaining up-to-date and relevant Customer Due Diligence data, documents and information so that the Branch can identify the changes in customer's risk profile. The following shall be followed by the Branch: -
 - (i) for customers who are rated as high risk, the Branch shall obtain updated CDD information (including updated copies of the customer's Officially Valid Documents if these have expired), as part of its periodic CDD review, or upon the occurrence of a trigger event as deemed necessary by the Branch, whichever is earlier; and
 - (ii) for all other risk categories of customers, the Branch should obtain updated CDD information upon the occurrence of a trigger event.
- (3) The Branch shall undertake a review under sub-clause (v) and (vii) of Clause 5.8, both periodically and at other appropriate times, including when:
 - (i) the Branch changes its CDD documentation requirements;
 - (ii) an unusual transaction with the customer is expected to take place;
 - (iii) there is a material change in the business relationship with the customer; or
 - (iv) there is a material change in the nature or ownership of the customer.

5.9. Ongoing Sanctions Screening

The Branch shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list when complying with Clause 5.4.1 (d).

5.10. Failure of Branch to conduct or complete customer due diligence

- (a) In cases where the Branch is unable to conduct or complete the requisite Customer Due Diligence for a customer in accordance with Clause 5.4.1, it, to the extent relevant, shall: -
- (i) not open an account or otherwise provide a service;
 - (ii) not carry out a transaction with or for the customer;

- (iii) not otherwise establish a business relationship;
- (iv) terminate or suspend any existing business relationship with the customer;
- (v) return any monies or assets received from the customer; and,
- (vi) consider whether the failure to conduct or complete Customer Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).

Provided that no application for onboarding or periodic updation of KYC shall be rejected, in case of Persons with Disabilities (PwDs), without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

- (b) The Branch is not bound to comply with sub-clauses (a) (i) to (v) above, if it amounts to “tipping off” of the customer, or FIU-IND directs the Branch to act otherwise.

Guidance Note: -

- (1) The Branch while complying under Clause 5.10(a), should apply one or more of the measures specified under sub-clauses (i) to (vi) above, as applicable, in the circumstances. In cases where CDD cannot be completed, it is appropriate that the Branch shall not carry out transaction until the completion of pending CDD.
- (2) Clause 5.10 shall apply to both existing and prospective customers. In case of existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances.
- (3) The Risk Based Approach shall be adopted for the Customer Due Diligence of the existing customers.

5.11. Periodic Updation

The Branch shall adopt a risk-based approach for periodic updation of CDD. The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows: -

- (i) Annually- for high-risk customers;
- (ii) once in three years- for medium risk customer; and,
- (iii) once in every five years- for low-risk customers.

Provided that the periodicity of such updation in case of resident Indian customer having an existing client relationship with the Financial Group in India, shall be as follows:

- (a) once in every two years - for high-risk customers,**
- (b) once in every eight years - for medium risk customers and**
- (c) once in every ten years - for low-risk customers.**

Provided further that where the risk categorization made by the Financial Group entity differs from the risk categorization made by the branch, the stricter of the two periodicity shall apply.

Explanation. - Policy in this regard shall be documented as part of Regulated Entity's

internal KYC policy, which is duly approved by the Governing Body of the Regulated Entity.

(a) **Individual Customers:**

(i) **No change in CDD information:**

In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Branch or through digital channels (such as online banking / internet banking, e-mail or mobile application of the Branch).

(ii) **Change in address:**

(aa) In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customer through customer's email-id registered with the Branch, customer's mobile number registered with the Branch, digital channels (such as online banking/ internet banking, e-mail or mobile application of the Branch). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

(bb) Further, the Branch shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the customer at the time of periodic updation.

(b) **Customers other than Natural Persons:**

(i) **No change in CDD information:**

In case of no change in the CDD information of a customer, which is a non-natural person, a self-declaration through email id registered with the Branch, digital channels (such as online banking / internet banking, mobile application of Branch), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the customer. Further, the Branch shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.

(ii) **Change in CDD information:**

In case of change in CDD information, the Branch shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

(c) **Additional measures:**

In addition to the above, the Branch shall ensure that:

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

- boarding a new customer.
- (ii) In case of Indian National, the customer's PAN details, if available with the Branch, is verified from the database of the issuing authority at the time of periodic updation of CDD.
 - (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 periodic updation. Further, the Branch shall ensure that the information / documents obtained from the customers at the time of periodic updation of CDD are promptly update its records / database and an intimation, mentioning the date of updation of CDD details, is provided to the customer.
 - (iv) The Branch shall adopt a risk-based approach with respect to periodic updation of CDD. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Branch (such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of CDD only where account is maintained, a more frequent periodicity of CDD updation than the minimum specified periodicity etc.), shall be clearly specified in its approved internal KYC policy.
 - (v) The Branch shall ensure that its internal KYC policy and processes on updation / periodic updation of CDD are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.
 - (vi) Branch 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 Branch 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 Branch's end.

6. THIRD PARTY RELIANCE

6.1. For the purposes of these Guidelines, “Third Party” shall mean-

- (a) A financial institution which is subject to and supervised by a financial regulator; or
 - (b) In relation to the Regulated Entity, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations;
- AND
- (c) Has an existing client relationship with a person whose data would be used for CDD and customer verification by a Regulated Entity.

6.2. The Branch may rely on a Third Party to perform CDD measures, subject to the following conditions:

- (a) The Branch shall obtain records or information of the client due diligence carried out by the third party, immediately;
- (b) The Branch shall take adequate steps to satisfy itself that the copies of identification data and other relevant documentation relating to the client

due diligence will be made available by the third party upon request, without delay;

- (c) The Branch is satisfied that the third party, it intends to rely upon, is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements mentioned under recommendation 10 and 11 of the FATF recommendations and also are in line with the requirements and obligations under the Act;

Provided that where the Branch relies on a third party that is part of the same Financial Group, the above condition is not applicable. The Branch can rely on member of the Financial Group subject to the condition that such member meets the following requirements: -

- (i) the Financial Group applies and implements a group-wide programmes on customer due diligence and record keeping, which meets the standards set out in the FATF Recommendations; and
 - (ii) the implementation of Customer Due Diligence and record keeping at the group level are supervised by a financial services regulator or other competent authority in a country.
 - (iii) The implementation of policies by groups. – Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003)- (3A).
- (d) The third party is not based in a country or jurisdiction assessed as high risk;
- (e) The Branch shall not rely on a third party to conduct ongoing monitoring of business relations with customers;
- (f) The Branch shall not rely on a third party specifically precluded by the Authority from relying upon;
- (g) The Branch shall document the basis for its satisfaction that the requirements under sub-clause 6.2.3 above, have been met;
- (h) The reliance on Third Party shall also be subject to the conditions that are specified in rule 9 (2) of the Rules and shall be in accordance with the regulations and circulars/guidelines issued by Authority from time to time; and,
- (i) The Branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

Guidance Note: -

- (1) In a Third-Party reliance scenario, the Third Party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with the relying Regulated Entity. The third party will

therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.

- (2) Obtaining records or information of the client due diligence under sub-clause 6.2.1 above, means obtaining all relevant CDD information, and not just basic information such as name and address.
- (3) For the avoidance of doubt, it is clarified that the Branch is not required automatically to obtain the underlying certified documents used by the third party to undertake its CDD. The Branch shall, however, under sub-clause 6.2.2 above, ensure that the certified documents are readily available from the third party on request.
- (4) The Branch shall take appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in.
- (5) Where a particular jurisdiction's laws (such as secrecy or data protection legislation) would prevent the Branch from having access to CDD information upon request without delay, the Branch should undertake the relevant CDD itself and should not rely on the third party.
- (6) If the Branch is not reasonably satisfied that a customer or Beneficial Owner has been identified and verified by a third party in a manner consistent with these Guidelines, the Branch shall immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.
- (7) When assessing under Clause 6.2(c) above, the Branch shall consider following factors including, among other things:
 - (i) mutual evaluations, assessment reports or follow-up reports published by FATF and other International Organisations;
 - (ii) contextual factors such as political stability or the level of corruption in the jurisdiction;
 - (iii) evidence of recent criticism of the jurisdiction, including in:
 - a) FATF advisory notices;
 - b) public assessments of the jurisdiction's AML regime by organisations referred to in (a); or
 - c) reports by other relevant non-government organisations or specialist commercial organisations.

7. CORRESPONDENT BANKING AND WIRE TRANSFERS

7.1. Correspondent Banking: The Branch shall have a policy approved by its Governing Body, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions namely: -

- (a) assessment of the suitability of the respondent bank by taking the following steps:

- (i) gather adequate information about the respondent bank to fully understand the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
- (ii) determine from the available sources, the reputation of the respondent bank and the quality of supervision over it, including whether it has been the subjected to any ML/TF investigation or regulatory action; and,
- (iii) assess the respondent bank's AML/CFT controls and ascertain whether they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;
- (b) the responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
- (c) obtain approval from the Senior Management before providing correspondent banking or similar services to a respondent bank.
- (d) in the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.
- (e) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
- (f) Correspondent relationship shall not be entered into with a bank which is a Shell Financial Institution.
- (g) It shall be ensured that the correspondent banks do not permit their accounts to be used by bank which is a Shell Financial Institution.
- (h) It shall be cautious with respondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
- (i) It shall be ensured 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.

7.2. Wire Transfers: This Clause shall apply to a Bank or Regulated Entity when it sends funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary, but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary, respectively.

7.2A The Branch shall verify the information pertaining to its customer where there is a suspicion of ML/TF.

7.2B All Financial Institutions shall transact and receive all monetary consideration (i.e. funds/fees/amount) only through an account

maintained with a Banking Unit in the IFSC.

- 7.3.** The Branch shall monitor payment messages to and from high-risk countries or jurisdictions, as well as transactions with high risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.
- 7.4.** Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, the Branch shall block, reject or freeze assets of these terrorists or terrorist entities immediately.
- 7.5.** Where there are positive hits arising from name screening checks, they should be escalated to the Principal Officer. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and be documented.
- 7.6.** The Branch shall not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another Regulated Entity in the payment process.

Guidance Note: -

- (1) Clause 7.2. is not intended to cover: -
- (i) any transfer that flows from a transaction carried out using a credit, charge, debit or prepaid card for the purchase of goods or services, so long as the credit, charge, debit or prepaid card number accompanies all transfers flowing from the transaction.
 - (ii) transfers and settlements between the entities, where both the originator and the beneficiary are Regulated Entities acting on their own behalf.
- (2) Clause 7.2. shall apply when a credit, charge, debit or prepaid card is used as a payment system to effect a person-to-person wire transfer. In such a case, the necessary information should be included in the message for such transactions.

7.7. Responsibility of the Ordering Institution

7.7.1. Identification and Recording of Information

Before effecting a wire transfer, every bank that is an ordering institution shall: -

- (a) identify the wire transfer originator and verify his or its identity; and
- (b) record adequate details of the wire transfer so as to permit its reconstruction, including but not limited to, the date of the wire transfer, the type and amount of currency transferred and the value date.

7.7.2. Cross-Border Wire Transfers Below or Equal to USD 1000

In a cross-border wire transfer where the amount to be transferred is below or equal to USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

- (a) the name of the wire transfer originator;
- (b) the wire transfer originator's account number (or unique transaction reference number where no account number exists);
- (c) the name of the wire transfer beneficiary; and
- (d) the wire transfer beneficiary's account number (or unique transaction reference number where no account number exists).

In a cross-border wire transfer where the amount to be transferred is equal to USD 1000, every bank which is an ordering institution shall also comply with the requirements specified under clause 7.7.3(a) of the guidelines. Clause 7.7.3(b) of the Guidelines shall apply to all Cross-Border Wire Transfers which are bundled in a batch file.

7.7.3. Cross-border Wire Transfers Exceeding or Equal To USD 1000

- (a) In a cross-border wire transfer where the amount to be transferred **is equal to or exceeds** USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the information required under Clause 7.7.2. (a) to (d), and any of the following:
 - (i) the wire transfer originator's residential address;
 - (ii) registered or business address, and if different, principal place of business, as the case may be;
 - (iii) the wire transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number); or
 - (iv) the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).
- (b) Where several individual cross-border wire transfers from a single wire transfer originator are bundled in a batch file for transmission to wire transfer beneficiaries, a bank shall ensure that the batch transfer file contains below information which are fully traceable within the beneficiary country:
 - (i) the wire transfer originator information required under Clause 7.7.3, which has been verified; and
 - (ii) the wire transfer beneficiary information required under Clause 7.7.3.

Clause 7.7.3(b) of the Guidelines shall apply to all Cross-Border Wire Transfers which are bundled in a batch file.

7.7.4. Domestic Wire Transfers

In a domestic wire transfer, every bank that is an ordering institution shall either:

- (a) include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

- (i) the name of the wire transfer originator;
- (ii) the wire transfer originator's account number (or unique transaction reference number where no account number exists); and
- (iii) any of the following:
 - (aa) the wire transfer originator's residential or registered or business address or principal place of business (if registered and business addresses are different), as applicable;
 - (bb) the wire transfer originator's unique national identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number);
 - (cc) the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).
- (b) Include only the wire transfer originator's account number (or unique transaction reference number where no account number exists), provided: -
 - (i) that these details will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary;
 - (ii) the ordering institution shall provide the wire transfer originator information set out in Clause 7.7.4.(a) above, within 3 business days of a request for such information by the beneficiary institution, by the Authority or other relevant authorities; and
 - (iii) the ordering institution shall provide the wire transfer originator information set out in Clause 7.7.4.(a) above, immediately upon request for such information by law enforcement authorities in India.
- (c) All wire transfer originator and beneficiary information collected by the ordering institution shall be documented. Where the ordering institution is unable to comply with the requirements under Clause 7.7.1. to 7.7.4, it shall not execute the wire transfer.

7.8. Responsibility of the Beneficiary Institution

- (a) **A bank that is a beneficiary institution shall take reasonable measures, including post event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack the required wire transfer originator or required wire transfer beneficiary information.**
- (b) **For cross-border wire transfers, a beneficiary institution shall identify and verify the identity of the wire transfer beneficiary, if the identity has not been previously verified.**
- (c) **A bank that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for determining:**
 - (i) when to execute, reject, or suspend a wire transfer lacking required information related to wire transfer originator or wire transfer beneficiary; and
 - (ii) the appropriate follow-up action.

7.9. Responsibility of the Intermediary Institution

- (a) A bank, who is acting as an intermediary institution, shall retain all the required information related to wire transfer originator and wire transfer beneficiary, accompanying the wire transfer.
- (b) Where technical limitations prevent the required information related to wire transfer originator or wire transfer beneficiary accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be preserved by the receiving intermediary institution for at least six years.
- (c) An intermediary institution shall implement appropriate internal risk-based policies, procedures and controls for determining-
 - (i) when to execute, reject, or suspend a wire transfer lacking required wire transfer originator or wire transfer beneficiary information; and
 - (ii) the appropriate follow-up actions including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.
- (d) The intermediary institution shall be required to take all reasonable measures, consistent with straight through processing, to identify cross border wire transfers that lack the information required under clause 7.7.6(a) of the Guidelines.

8. INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

8.1. Internal Policies

The Branch shall develop and implement adequate internal policies, procedures, and controls, taking into consideration its ML/TF risks and the size of business, to help prevent ML/TF, and communicate these to its employees.

Guidance Note:

As internal policies and procedures serve to guide employees, officers and representatives in ensuring compliance with AML/CFT laws and regulations, it is important that the Branch updates its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

8.2. Compliance

- (a) The Branch shall develop appropriate compliance management, including appointing or designating a Principal Officer at the management level and shall also develop compliance framework.

- (b) The Branch shall ensure that the Principal Officer, as well as any other persons appointed to assist him, is suitably qualified and, has adequate resources and timely access to all customer records and other relevant information which he may require to discharge his functions.
- (c) The Branch shall ensure that the Principal Officer has the necessary seniority and authority within the Branch to effectively perform his responsibilities.
- (d) The responsibilities of the Principal Officer shall include:
 - (i) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with these Guidelines;
 - (ii) promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organisation;
 - (iii) informing employees, officers and representatives promptly of regulatory changes;
 - (iv) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
 - (v) reporting or overseeing the reporting of suspicious transactions;
 - (vi) advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;
 - (vii) reporting to Senior Management on the outcome of reviews of the Branch's compliance with these Guidelines & risk assessment procedures; and
 - (viii) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Branch's Senior Management.
- (e) The business interests of the Branch should not interfere with the effective discharge of the above-mentioned responsibilities of the Principal Officer and potential conflicts of interest should be avoided.
- (f) To enable unbiased judgments and facilitate impartial advice to management, the Principal Officer should be distinct from the internal audit and business line functions. Where any conflict between business lines and the responsibilities of the Principal Officer arises, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the Branch's management.

8.3 AUDIT

- (a) The branch shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the branch's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines.
- (b) The branch's AML/CFT framework should be subjected to periodic audits. Such

audits should be performed not just on individual business functions but also on the branch-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would inter-alia include-

- (i) Determining the adequacy of the branch’s AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;
- (ii) Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee’s, officer’s and representative’s compliance with established AML/CFT policies and procedures; and
- (iii) Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the branch’s business.

8.4 Training and awareness

The Branch shall: -

- (a) provide AML/CFT training to all relevant employees, periodically;
- (b) ensure that its AML/CFT training enables its employees to:
 - (i) comprehend the applicable laws relating to ML/TF, including the Act and Rules;
 - (ii) understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;
 - (iii) recognise and deal with transactions and other activities which may be related to ML/TF;
 - (iv) comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
 - (v) have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of the Branch;
 - (vi) understand their roles and responsibilities in combating ML/TF, including the identity and duties of the Principal Officer and deputy, where applicable; and,
 - (vii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Clause 6.
- (c) ensure that its AML/CFT training:
 - (i) is relevant and tailored to the Branch’s activities, including its products, services, customers, distribution channels, business

partners, level and nature of its transactions; and

- (ii) identifies and indicates the different levels of ML/TF risk and vulnerabilities associated with the matters in sub-clause (c)(i) above.

Guidance Note: -

- (1) All new relevant employees of the Branch should be given appropriate AML/CFT training as soon as reasonably practicable after commencing employment with the Branch.
- (2) The manner of providing AML/CFT training may not necessarily be formal and may include any medium which is considered appropriate.
- (3) A relevant employee may include a member of the Senior Management or operational staff, any employee with customer contact or who handles or may handle customer monies or assets, and any other employee who might otherwise encounter ML/TF in the business context.

9. Record Keeping

9.1. The Branch shall maintain the following records:

- (a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
- (b) records of customer business relationships (both original and certified copies), which include: -
 - (i) correspondence of business and other information relating to a customer's account;
 - (ii) adequate records of transactions to enable standalone transactions to be reconstructed; and
 - (iii) internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;
- (c) notifications made under Clause 10.1.(b);
- (d) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;
- (e) any relevant communications, if made with the FIU;
- (f) the documents referred to in Clause 9.4; and
- (g) any other matter that the Branch may be expressly required to record and maintain, under these Guidelines.

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.

- 9.2.** The Branch shall preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed.
- 9.3.** The Branch shall provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines.

9.4. Risk Assessment Documents

The Branch shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including: -

- (a) the business risk assessment undertaken by them as per Clause 3.1;
- (b) how the business risk assessment in (a) was used for the purposes of complying with Clause 4.1.(a);
- (c) the risk assessment of its customer undertaken under Clause 4.1.(a) (i); and,
- (d) the determination of risk rating made under Clause 4.1.(a) (ii).

Guidance Note: -

- (1) The Branch shall comply with the requirements prescribed under rule 3, 4 and 5, along with any other applicable provisions under the Act, Rules and these Guidelines.
 - (2) The above records may be kept in electronic format, subject to the condition that such records are readily accessible and promptly made available to the Authority or other law enforcement agency, on demand.
 - (3) Where the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.
 - (4) The Branch shall evolve a system for proper maintenance and preservation of records in such a manner that allows:
 - (a) data to be retrieved easily and quickly whenever required or when demanded by the competent authorities;
 - (b) the Authority or any other competent authority is able to assess the Branch's compliance with the applicable laws;
 - (c) identification of a customer or third party;
 - (d) it permits reconstruction of any transaction which was processed by or through the Branch on behalf of a customer or other third party.
- 9.5.** Where the records referred to in Clause 9.1 are kept by the Branch outside the IFSC, the Branch shall:
- (a) take all reasonable steps to ensure that the records are kept in a manner

consistent with these Guidelines;

- (b) ensure that the records are easily accessible to it; and
- (c) ensure that the records are immediately made available for inspection, when so desired by the Authority.

9.6. The Branch shall:

- (a) verify if there are secrecy or data protection laws that would restrict access without delay to the records referred to in Clause 9.1, by the Regulated Entities, the Authority or the law enforcement agencies of India; and
- (b) where such law exists, obtain without delay, the certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons referred in Clause (a) above.

9.7. The Branch shall be able to convey that they have complied with the training requirements in Clause 8 through appropriate measures, including the maintenance of relevant training records.

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

10. PROCESS OF IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

10.1. Internal reporting requirements

- (a) The Branch shall establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/TF.
- (b) The Branch shall put in place such policies, procedures, systems and controls which ensure that whenever any of its employee, acting in the ordinary course of his employment, either:
 - (i) knows;
 - (ii) suspects; or
 - (iii) has reasonable grounds for knowing or suspecting; that a person is engaged in or attempting ML/TF, that employee promptly notifies the Principal Officer of the Branch with all relevant details.

10.2. Indications of Suspicious Transactions

The Branch can identify suspicious transactions by following these four steps:

- (a) Detect a suspicious indicator(s);
- (b) Ask the customer questions;

- (c) Review customer's records; and
- (d) Evaluate the above information.

(a) Detect Suspicious indicators

The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity or lacks a business or apparent lawful purpose.

Guidance Note: -

- 1) The suspicious indicators act as "red flags" and alerts for the Branch to pay more attention to a particular customer or transaction(s). These indicators include:
 - (a) complex, unusual or large transactions that have no apparent economic or lawful purpose;
 - (b) unusual pattern of transactions that have no apparent economic or lawful purpose;
 - (c) the transaction (or attempted transaction) does not match the known background, nature and type of customer, including source of funds;
 - (d) unusual customer behaviour;
 - (e) Customers whose identity verification seems difficult or clients that appear non-cooperative;
 - (f) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
 - (g) Customers based in high-risk jurisdictions;
 - (h) Substantial increases in business without apparent cause; or
 - (i) Attempted transfer of investment proceeds to apparently unrelated third parties.
- 2) The presence of suspicious indicators does not immediately equate to the criminality or suspicion. Rather, the detection of an indicator especially a combination of indicators should prompt the Branch to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU-IND as suspicious.

(b) Ask Customer Questions

- (i) If one or more suspicious indicators are detected, the Branch and its employees may ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.
- (ii) The Branch shall ensure that when asking such questions, they do not "tip-off" the customer. Instead, questions could be asked using a service approach.

(c) Review Customer's Records

The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. To achieve this, the Branch shall review its customer's records and consider all information that is already known to it about the customer. This may include:

- (i) the customer's usual occupation, business or principal activity;
- (ii) the customer's transaction history;
- (iii) the customer's risk profile;
- (iv) the customer's income level;
- (v) the customer's source of income as stated during account opening or initial engagement;
- (vi) reasons for the transactions as provided by the customer;
- (vii) the “relationship” of the customer with the sender or beneficiary of funds;
- (viii) the frequency of transactions;
- (ix) the size and complexity of the transaction;
- (x) the identity or location of any other person(s) involved in the transaction;
- (xi) the usual or typical financial, business or operational practices or behaviour of customers in the similar occupation or business category; and
- (xii) the availability of identification documents and other documentation.

After reviewing as aforesaid if the Branch finds that the customer's profile has changed, it shall update the customer's profile.

(d) Evaluate Information Collected

(a) The Branch shall evaluate the:

- (i) suspicious indicators,
- (ii) information solicited from the customer through questions asked, and
- (iii) known information about the customer to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence.

(b) If the Branch concludes that there are reasonable grounds to suspect that the transaction(s) or attempted transaction(s) is linked to a ML/ TF or any other serious offence, it should report this suspicion to the FIU-IND by completing and submitting a STR.

Guidance Note: -

- 1) The Branch should be able to clearly articulate the reasons for its suspicion based on this evaluation. If the Branch is unable to establish reasonable grounds of

suspicion, it must continue monitoring the customer or the business relationship.

- 2) By monitoring a customer’s activity, the Branch may revert to any of the above steps (detect, ask, review and evaluate) at a later date and find that new facts and context may raise the suspicion to meet the reasonable grounds of suspicion threshold.
- 3) The requirement to report any suspicious transaction applies to all types of transaction. There is no minimum monetary threshold amount for reporting suspicious transactions. Thus, a transaction considered suspicious should be reported to the FIU-IND regardless of the currency or amount of the transaction.
- 4) If the Branch is not able to obtain satisfactory evidence of a customer’s identity, the Branch should not proceed further with the transaction unless directed in writing to do so by the FIU-IND.
- 5) If the Branch considers the reasons for the customer’s failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it shall report the attempted transaction to the FIU-IND as a suspicious transaction.

10.3. REPORTING OF SUSPICIOUS TRANSACTIONS

Reporting Requirements to Financial Intelligence Unit – India

(1) The name, designation and address of the Designated Director and the Principal Officer shall be communicated by the branch to the FIU-IND and the Authority.

(2) The branch shall furnish to the Director, Financial Intelligence Unit-India (FIUIND), the required information referred to in rule-3 of the Rules and in accordance with the terms of rule-7 thereof..

Guidance Note: -

- 1) The reporting formats and comprehensive reporting format guide prescribed or released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist the Branch in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file Suspicious Transaction Reports (STR) which FIU-IND has placed on its website, shall be made use of by Branch which are yet to install/adopt suitable technological tools for extracting STR from their live transaction data.
 - 2) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.
- 2A) Branch shall not restrict any transaction in any account merely on the basis of the STR file.**
- 3) Robust software to throw alerts when the transactions are inconsistent with risk

categorization and updated profile of the customers, shall be put in to use as a part of effective identification and reporting of suspicious transactions.

- 4) In terms of the Rules, the Branch is mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND)
- 5) The Branch shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND.
 - (a) Further, in terms of Rules, the Branch shall inter-alia adhere to the following:
 - (i) The Suspicious Transaction Report (STR) shall be submitted promptly on conclusion that any transaction or a series of transactions that are integrally connected, are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
 - (ii) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
 - (iii) The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND;
 - (iv) Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND.

10.4 Confidentiality of Suspicious Transaction Report (STR)

- (a) The Branch and its employees or agents shall not disclose to any person (including the customer);
 - (i) that it has reported or will be reporting a suspicious transaction to the FIU-IND;
 - (ii) that it has formed a suspicion on a particular customer's transaction; or
 - (iii) any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU-IND.
- (b) Disclosure of information on suspicious transactions is only allowed under the following circumstances:
 - (i) disclosure to an officer, employee or agent of the Regulated Entity for any purpose connected to the performance of that person's duties;
 - (ii) disclosure to a lawyer for the purpose of obtaining legal advice on the matter;
 - (iii) disclosure to a supervisory authority (to enable it to carry out its supervisory role); or

- (iv) disclosure in compliance with the court order; or
- (v) disclosure or information sharing among entities in a Financial Group.
- (c) The Branch and its employees are protected from any civil, criminal or disciplinary action taken against them for reporting a suspicious transaction in good faith.

Guidance Note:

- 1) No Nil reporting needs to be made to FIU-IND in case there are no suspicious/non – profit organization transactions to be reported. The Branch shall not put any restrictions on operations in the accounts where an STR has been made. The Branch and its employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND.
- 2) This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the customer at any level.
- 3) It is clarified that the Branch, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of the Schedule of the Act, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

10.5 Additional measures

- (a) Lawyers, notaries, Chartered Accountants, Company Secretaries, Cost and Works Accountants and entities offering such services shall report suspicious transactions when, on behalf of or for a 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) Individuals 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;

Explanation.– For removal of doubts, it is clarified that the following activities shall not be regarded as activity for the purposes of sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the Act, namely:-

- (a) any activity that is carried out as part of any agreement of lease, sub-lease, tenancy or any other agreement or arrangement for the use of land or building or any space and the consideration is subjected to deduction of income-tax as defined under section 194-I of Income-tax Act, 1961 (43 of 1961); or
- (b) any activity that is carried out by an employee on behalf of his employer in the course of or in relation to his employment; or
- (c) any activity that is carried out by an advocate, a chartered accountant, cost accountant or company secretary in practice, who is engaged in the formation of a company to the extent of filing a declaration as required under clause (b) of sub-section (1) of section 7 of Companies Act, 2013 (18 of 2013); or
- (d) any activity of a person which falls within the meaning of an intermediary as defined in clause (n) of sub-section (1) of section 2 of the Prevention of Money-laundering Act, 2002 (15 of 2003).

11. COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

11.1. Requirements/obligations under International Agreements Communications from International Agencies –

- (a) The Branch shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) 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:
 - (i) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-

Qaida Sanctions List is available at:

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

- (ii) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at:

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

- (b) Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available at https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf
- (c) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.
- (d) The Regulated Entity shall adhere to the countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

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

The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed and compliance with the Order shall be ensured. Order dated 2nd February 2021, as amended vide Corrigendum No. 14014/01/2019/CFT-83 dated 15th March 2023, is further modified through a Corrigendum dated 29th August 2023 by the CFT Cell/ CTCR Division of the Ministry of Home Affairs, Government of India. Which are available on the website of Ministry of Home Affairs. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs

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

The Branch 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 **01 September 2023** which is available at https://fiuindia.gov.in/pdfs/AML_legislation/DoR_Section_12A_WMD.pdf and further as amended from time to time. It has been clarified that the sanctions against any person or entity shall be imposed 'without

delay' i.e. on the same business day but not later than 24 hours in any case.

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

(a) FATF Statements circulated from time to time, and publicly available information for identifying countries which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

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

Explanation: *The process referred to in (a) and (b) above, do not preclude the Branch 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 as aforesaid shall be examined, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

11.5. Secrecy Obligations and Sharing of Information:

- (a) The Branch shall maintain secrecy regarding the customer information that arises out of the contractual relationship between it and the customer.
- (b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express consent of the customer.
- (c) While considering the requests for data/information from Government and other agencies, the Branch shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.
- (d) The exceptions to the above obligations shall be as under:
 - (i) Where disclosure is under compulsion of law;
 - (ii) Where there is a duty to the public to disclose;
 - (iii) Where the interest of Bank requires disclosure; and
 - (iv) Where the disclosure is made with the express or implied consent of the customer.

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

Under FATCA and CRS, the Branch shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and shall take following steps for complying with the reporting requirements:

- (a) Register on the related e-filing 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: The Branch shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <https://fedai.org.in/> 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>. The Branch shall also take note of the following:
 - (i) updated Guidance Note on FATCA and CRS; and
 - (ii) a press release on 'Closure of Financial Accounts' under Rule 114H.

11.7. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR):

(a) In terms of provision of rule 9(1A) of Rules, the Branch shall capture customer's KYC records and upload on CKYCR within 10 days of commencement of an account-based relationship with the customer in the form and manner as prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) and shall ensure that:

- (i) the KYC records to be uploaded are as per KYC Template released by CERSAI.
- (ii) Once KYC Identifier is generated by CKYCR, the same is communicated to the Customer.
- (iii) It has performed the last KYC verification or has sent updated

information in respect of a Customer to CKYCR.

- (b) For the purpose of establishing an account-based relationship or for verification of identity of a customer or for undertaking on-going due diligence, the Regulated Entity 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 applicable KYC norms under these Guidelines; or,**
 - (iii) the validity period of the downloaded documents has lapsed; or.**
 - (iv) the Regulated Entity 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.”**
- (c) Whenever the Regulated Entity obtains additional or updated information from any customer as per clause (b) above, it shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall then update the existing KYC records of such customer.**
- (d) The CKYCR shall thereafter inform electronically all the Regulated Entities who have dealt with the concerned customer regarding updation of KYC record of such customer and on receipt of such information, the concerned Regulated Entity shall retrieve the updated KYC records from CKYCR and update the KYC records maintained by them.**
- (e) The Regulated Entities engaged in the following activities shall adhere to the requirements stipulated under sub-clause (a) to (d) above:**
- (i) Payment Service Provider;**
 - (ii) Finance Company undertaking core activities (Finance Company-Core);**
 - (iii) IFSC Banking Unit;**
 - (iv) Bullion Trading /Clearing Member;**
 - (v) Broker Dealer;**
 - (vi) Clearing Member;**
 - (vii) Depository Participant;**
 - (viii) Investment Advisor;**

- (ix) Fund Management Entity;
- (x) General Insurance;
- (xi) Life Insurance.”

Guidance Note

1) Under rule 9A of the Rules, the branch shall submit KYC Records to the CKYCR, in case of the Indian nationals. However, such requirement shall not be applicable for a client who is a foreign national.

(2) Notwithstanding anything provided above, where the branch intends to submit the KYC records of a foreign national to the CKYCR, in such case the documents issued by the Government departments of foreign jurisdictions and letters issued by the Foreign Embassy or Mission in India shall be accepted as proof of current address and when this proof of address is accepted, then any of the following OVDs shall be obtained as the proof of identity and address:

- (i) Passport;
- (ii) Driving License; or
- (iii) Voter Identity Card..

12. 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

Guidance on CDD Procedure

Part-I

Guidance for identification of the customers

For on-boarding customers, the Branch may obtain such information as may be required under these Guidelines, in addition to that is required under the Act and Rules. The Illustrative list of information to be obtained for on-boarding customers is provided below: -

(1) For Individual

- (i) Full name, including any aliases;
- (ii) Unique Identification Number (such as an Identity card number, passport number, etc.);
- (iii) Date of birth;
- (iv) Nationality;
- (v) Legal domicile;
- (vi) Current residential address; (other than a post office box address);
- (vii) Contact details such as personal, office or work telephone numbers.
- (viii) Occupation or profession, name of employer and location of activity; (wherever applicable)
- (ix) Information regarding the nature of the business to be conducted; (wherever applicable)
- (x) Information regarding the origin of the funds; and (wherever applicable)
- (xi) Information regarding the source of wealth or income. (wherever applicable).

Guidance Note

The address of a customer should enable the Branch to physically locate the customer.

(2) For Legal Person or Legal Arrangement

In cases where the customer is a legal person or legal arrangement, the Branch shall, apart from identifying the customer, shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. Additionally, the Branch shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, the Branch shall obtain the following information of each related or connected party:

- (i) full name, including any aliases; and
- (ii) Unique Identification Number (such as an Identity card number,

passport number, etc.).

Part-II

Guidance for verification of the identity of the customers

(1) Verification of identity through following documents:

- (i) Passport;
- (ii) Driving license;
- (iii) Proof of possession of Aadhar number (for Indian Nationals);
- (iv) Voter's Identity Card issued by Election Commission of India (for Indian Nationals);
- (v) For foreign nationals, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as OVD.

Explanation 1: Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by the branch.

Explanation 2: 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, 2016 and the regulations made thereunder

(2) where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be OVD:

- (i) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- (ii) letter issued by a gazetted officer, with a duly attested photograph of the person.

(3) The Branch shall ensure that any document used for the purpose of verification of the identity of the customer is an original document.

(4) In case a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where the Branch has no physical contact with the customer, or the on boarding of customer is done through non-face to face mode); the Branch should obtain a copy of the OVD that is certified to be a 'true copy' and such certification may be carried out by any one of the following: -

- (i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking

relationship;

- (ii) Notary Public (outside India);
- (iii) Court Magistrate (outside India);
- (iv) Judge (outside India);
- (v) Certified public or professional accountant (outside India);
- (vi) Lawyer (outside India);
- (vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or
- (viii) any other authority as may be specified by the Authority.

(5) The person certifying the OVD should be contactable.

(6) Where certification of an OVD is done by the authorised officer of the Branch, such certified copy should be dated, signed and marked with 'original sighted/verified'.

(7) Where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document shall also be deemed to be Officially Valid Document:

- (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, Municipal tax receipt, city council tax receipt, or such other equivalent document;
- (iii) bank account or Post Office savings bank account statement or statement of foreign bank; (applicable only for low-risk customers)
- (iv) pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- (v) 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; and

Provided also that in case the OVD presented by a foreign national does not contain the details of address, 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.

(8) **The illustrative list of documents or the equivalent e-documents thereof, which may be obtained for verification of the identity of Legal Person or Legal Arrangement, are as follows:**

(i) In case of Company

- (a) Certificate of incorporation;
- (b) Memorandum and Articles of association;
- (c) PAN or equivalent document prevalent in the home jurisdiction of the company;
- (d) A resolution passed by the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf;
- (e) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the company.
- (f) The names of the relevant persons holding senior management position; and
- (g) The registered office and the principal place of its business, if it is different.

(ii) In case of Partnership/limited liability partnership

- (a) Registration certificate;
- (b) Partnership deed/limited liability partnership deed;
- (c) PAN or equivalent document prevalent in the home jurisdiction of the partnership firm;
- (d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the partnership firm;
- (e) Such other documents as may be required by the Branch to collectively establish the existence of such partnership firm.
- (f) The names of all the partners and
- (g) Address of the registered office, and the principal place of its business, if it is different.

(iii) In case of Trust

- (a) Registration certificate;
- (b) Trust deed;
- (c) PAN or equivalent document prevalent in the home jurisdiction of the trust;
- (d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Trust.
- (e) the names of the beneficiaries, trustees, settler, protector, if any and authors of the trust.
- (f) the address of the registered office of the trust; and
- (g) list of trustees and documents, as are required for verification of the identity of Individuals for those discharging role as trustee and authorized to transact on behalf of the trust.

(iv) In case of Unincorporated Associations/ Bodies

- (a) Resolution of the managing body of such association/body;
- (b) PAN or equivalent prevalent document in the home jurisdiction;
- (c) Power of attorney granted to transact on its behalf;
- (d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transaction on behalf of the Unincorporated Associations/ Bodies;
- (e) Such other documents as may be required by the Branch to collectively establish the existence of such association/body.

(v) For opening account of a customer who is a juridical person (not specifically covered in the earlier part)

When the client purports to act on behalf of juridical person or individual or trust, the Branch shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

Provided that in case of a trust, it shall be ensured that trustees disclose their status at the time of commencement of an account based relationship or when carrying out following transactions: -

1. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.
2. 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.
3. 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.

Part-III

Various modes of verification of the identity of the customers

- (i) Use of Business Facilitators;
- (ii) Except for high-risk customers, the following mode of verification may also be considered: -
 - (a) downloading publicly available information from an official source (such as a regulator's or other official government website).
 - (b) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases may also be acceptable as a reliable source, provided that the commercial database

is recognized for such purpose by the home regulator.

Guidance Note on Business Facilitator: -

- 1) The Branch may identify the Business Facilitators in different geographies and shall sign agreements with them with specific terms and conditions ensuring customer secrecy and data protection.
- 2) The Branch shall maintain the details of the Business Facilitators assisting the customer, where such services are utilized. The ultimate responsibility for customer due diligence will always be with the Regulated Entities.
- 3) The Branch will use Business Facilitators for verifying the information/OVD provided by the customer for opening account.
- 4) The Business Facilitators shall be domiciled and regulated or registered in jurisdiction not identified in the public statement of FATF as ‘High Risk Jurisdictions’ subject to a ‘Call for Action’; or from any country specified by the Government of India by an order or by way of agreement or treaty with other sovereign governments.

Annexure-II

PART-A

V-CIP PROCESS FOR ONBOARDING INDIAN NATIONALS

1.1. Branch may undertake V-CIP to carry out:

- (a)** CDD in case of on-boarding of new customers such as an individual, proprietor (in case of a proprietorship firm), authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer.
- (b)** Updation/Periodic updation of KYC for eligible customers.

1.2. While undertaking V-CIP, the Branch shall adhere to the following minimum standards:

1.2.1.V-CIP Infrastructure

- (i) The branch shall comply with the minimum baseline cyber security and resilience framework namely, "Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs" dated March 10, 2025 (as amended from time to time), issued by the Authority and all other applicable laws on mitigating or managing Information Technology risks.
- (ii) The technology infrastructure for V-CIP shall be housed within the premises of the branch or its Financial Group supervised by a financial regulator or a KYC Registration Agency(KRA); and the connections and interactions for undertaking V-CIP shall originate from its own secured network domain.
- (iii) Any technology related outsourcing for the process shall be compliant with the standards, as may be specified by the Authority.
- (iv) Where cloud deployment model is used, the branch shall ensure that the ownership of data in such model rests only with the branch or its Financial Group.
- (v) Further, the branch shall also ensure that all such data including video recordings are transferred to the server(s)/cloud server owned or taken on lease by the Regulated Entity or its Financial Group, 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 branch.

Explanations:

Explanation I : In case the technology infrastructure is housed outside India with the Financial Group, the branch shall immediately inform the Authority;

Explanation II : In case the data, including video recordings, are transferred to the server(s) or cloud server owned or taken on lease by its Financial Group, the branch shall have access to such data.

- (vi) The branch shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application/digital platform, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(vii) The V-CIP infrastructure/application should be capable of preventing the connections from spoofed IP addresses, using VPNs or proxy servers.

Explanation. – For removal of doubt, it is hereby clarified that for resident Indian customers, the IP address shall emanate from India and for Non-Resident Indian it shall emanate either from India or from any one of the following countries where he or she is resident:

- a) United States of America;
- b) Japan;
- c) South Korea;
- d) United Kingdom excluding British Overseas Territories;
- e) Canada;
- f) UAE;
- g) Singapore;
- h) Australia.
- i) European Union excluding Croatia

Provided that the aforementioned jurisdictions shall not be identified by FATF as High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring or by Central Government as high risk jurisdiction for money laundering, terrorist financing or proliferation financing.

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

(ix) 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 branch. Appropriate artificial intelligence (AI) technology with randomness and anti-deep fake and anti-fraud checks must be used to ensure that the V-CIP is robust.

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

(xi) 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) or any such other suitably accredited agencies as may be specified. Such tests should also be carried out periodically in conformance to internal /

regulatory guidelines

(xii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance and 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.

1.2.2.V-CIP Procedure

(i) Branch shall formulate a clear policy, workflow and standard operating procedure for V-CIP and ensure adherence to it.

(ii) The V-CIP process shall be operated only by officials of the branch or financial group entity in India supervised by a financial regulator or a KRA Registration Agency under an agreement with specific terms and conditions ensuring customer secrecy and data protection. The branch will be ultimately responsible for customer due diligence.

(iii) The official should be specially trained for this purpose and capable of carrying out liveness check and detect deep-fakes, any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.

(iv) 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 branch. However, in case of call drop / disconnection, fresh session shall be initiated.

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

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

(vii) 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 workflow.

(viii) The authorised official of the branch 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) Offline Verification of Aadhaar for identification;
- (b) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer,
or KYC Registration Agency (KRA) set up in IFSC;
- (c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.
- (d) Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by RE.

(ix) A Regulated Entity shall redact or blackout the Aadhaar number in the manner as provided under Part B of Annexure II.

(x) 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.

(xi) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Regulated Entities shall ensure 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, the Regulated Entities shall ensure that no incremental risk is added due to this.

(xii) 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.

(xiii) The branch shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified online from the database of the issuing authority including through Digilocker. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP. Where a customer does not hold a PAN, an (the Circular can be accessed at <https://shorturl.at/XDIH4>).thereof shall be obtained.

(xiv) The authorised official of the Regulated Entity 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.

(xv) 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.

(xvi) All matters not specified under the above clauses but required under other statutes such as the Information Technology (IT) Act and the Digital Personal Data Protection Act, 2023 or the rules and regulations made thereunder, shall be appropriately complied with by the branch.

1.2.3.V-CIP Records and Data Management

(i) The branch shall ensure that the video recordings are 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 these Guidelines, shall also be applicable for V-CIP;

(ii) The activity logs along with the credentials of the authorised person of the branch performing the V-CIP shall be preserved.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) Customers (classified as low-risk) through V-CIP

(i) The Regulated Entities may onboard customers, who are Non- Resident Indian ('NRI Customers'), through V-CIP to carry out:

(a) CDD in case of on-boarding of new customers such as individual, proprietor in case of proprietorship, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer;

(b) Updation/Periodic updation of KYC.

Explanations. –

Explanation I: For the purposes of this part, the term “NRI customer” shall refer to a Non-Resident Indian who has been classified as a low-risk customer, by the Regulated Entity in accordance with these Guidelines, and resides in any of the following jurisdictions:

- a) United States of America;
- b) Japan;
- c) South Korea;
- d) United Kingdom excluding British Overseas Territories;
- e) Canada;
- f) UAE;
- g) Singapore;
- h) Australia;
- i) European Union excluding Croatia

Explanation II: For the avoidance of doubt, it is hereby clarified that the branch shall undertake V-CIP only for NRI customers residing in any of the above specified jurisdictions and submits valid proof of current address to that effect.

- (ii) While undertaking the V-CIP for on-boarding the NRI customers, the branch shall ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted to the branch.
- (iii) The branch shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction specified in *Explanation 1* above, for the purpose of verification of the current address.
- (iv) Upon verification of the proof of identity of the NRI Customer, in cases where current address of NRI customer cannot be verified from reliable/issuing authority sources, the Regulated Entity shall open the account of the customer in the debit freeze / inactive mode; and shall communicate such customer the manner of activation of debit freeze / inactive account.
- (v) The said debit freeze / inactive account of the NRI Customer shall be made operational only upon the receipt and verification of first credit from the bank account provided by such customer as proof of current address at the time of V-CIP on-boarding process..

PART-B

DIGITAL KYC PROCESS FOR INDIAN NATIONALS

For undertaking CDD of Indian nationals, the branch 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) the customer decides to submit his Aadhaar number voluntarily to the branch notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(bb) 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 the customer's identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof, as defined in Income-tax Rules, 1962; and

(c) 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 branch:

Provided that where the customer has submitted

(i) Aadhaar number under Clause (a) above, to the branch notified under first proviso to sub-section (1) of section 11A of the Act, and branch shall carry out authentication of the customer's Aadhaar number 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, he may give a self-declaration to that effect to the branch.

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

(iii) an equivalent e-document of any OVD, the Regulated Entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under digital KYC Process as specified under Annexure I of Rules.

(iv) any OVD or proof of possession of Aadhaar number under (a)(i)(bb) above where

offline verification cannot be carried out; the branch shall carry out verification through digital KYC Process as specified under Annexure I of Rules.

Provided that for a period not beyond such date as may be notified by the Government

for a class of Regulated Entities, instead of carrying out digital KYC, the branch 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.

Explanation I: Branch shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

Explanation II: Biometric based e-KYC authentication can be done by authorised official of the branch.

Explanation III: 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, 2016 and the regulations made thereunder.

ਪੰਜਾਬ ਨੇਸ਼ਨਲ ਬੈਂਕ
ਡੇਟਾ ਪ੍ਰਾਇਵੇਸੀ ਏਵਾਂ ਪ੍ਰਬੰਧਨ ਪ੍ਰਭਾਗ, ਪ੍ਰਧਾਨ ਕਾਰਜਾਲਯ
PUNJAB NATIONAL BANK
DATA PRIVACY & MANAGEMENT DIVISION, HEAD OFFICE

*“Confidential
Strictly for internal Circulation Only”*

Annexure- III

INDEX OF ABBREVIATIONS

S.N.	Abbreviation	Full form
1	AML/CFT	Anti-Money Laundering/Countering of Terrorist Financing (also used for <i>Combating the financing of terrorism</i>)
2	BF	Business facilitator
3	BO	Beneficial Owner
4	CDD	Customer Due Diligence
5	CKYCR	Central Know Your Customer Records Registry
6	CRS	Common Reporting Standards
7	ECDD	Enhanced Customer Due Diligence
8	FATCA	Foreign Account Tax Compliance Act
9	FATF	Financial Action Task Force
10	FIU-IND	Financial Intelligence Unit- India
11	KYC	Know Your Customer
12	IFSCs	International Financial Services Centres
13	IFSCA	International Financial Services Centres Authority
14	ML/TF	Money Laundering/Terrorist Financing
15	NPO	Non-Profit Organisation
16	NRI	Non- Resident Indian
17	OVD	Officially Valid Document
18	PEP	Politically Exposed Person
19	RBA	Risk-Based Approach
20	RE	Regulated Entity
21	SCDD	Simplified Customer Due Diligence
22	STR	Suspicious Transaction Report
23	V-CIP	Video- Customer Identification Procedure
24	NTR	Non-Profit Transaction Report
25	UAPA	Unlawful Activities (Prevention) Act, 1967
26	UNSC	United Nations Security Council