



**POLICY ON  
KNOW YOUR CUSTOMER (KYC),  
ANTI MONEY LAUNDERING (AML) MEASURES  
AND  
COMBATING FINANCING OF TERRORISM (CFT)**

**Version 8.1**

## Table of Contents

Table of Contents .....	2
1. Short Title .....	4
2. Objective .....	4
3. Applicability .....	5
4. Definitions.....	5
5. The KYC policy includes the following four key elements: .....	17
6. Money Laundering and Terrorist Financing Risk Assessment by Bank .....	17
7. Compliance with KYC policy:.....	17
8. Customer Acceptance Policy (CAP).....	18
9. Risk Perception in respect of Customer:.....	20
10. Customer Identification Procedure (CIP) .....	22
11. Customer Due Diligence requirements while opening accounts .....	23
12. Basic Savings Bank Deposit Accounts.....	33
13. Account opened using OTP based e-KYC, in non-face-to-face mode .....	35
14. Accounts of Foreign students studying in India: .....	37
15. Accounts of Politically Exposed Persons (PEPs) resident outside India .....	38
16. Accounts of persons other than individuals:.....	39
17. CDD Measures for Sole Proprietary firms.....	39
18. CDD Measures for Legal Entities.....	40
19. Identification of Beneficial Owner .....	43
20. On-going Due Diligence .....	44
21. Periodic updation of KYC .....	45
22. Miscellaneous .....	48
23. Issue of Demand Drafts, etc., for more than Rs. 50,000/- .....	49

24. Unique Customer Identification Code .....	50
25. Monitoring of Transactions: .....	50
26. Risk Management: .....	52
27. Record Management .....	61
28. Combating Financing of Terrorism (CFT) .....	62
29. Reporting Requirements .....	66
30. General Guidelines: .....	68
31. Annexure 1 .....	79
32. Annexure 2 .....	79
33. Annexure 3 .....	81
34. Annexure 4 .....	83
35. Annexure 5 .....	83
36. Annexure 6 .....	111
37. Annexure 7 .....	125

## 1. **Short Title**

Policy guidelines on Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) Measures / Obligation of the Bank under Prevention of Money Laundering Act (PMLA), 2002 shall be called as Know Your Customer – Anti Money Laundering (KYC-AML) Policy, Version 8.1.

## 2. **Objective**

The objective of the Policy is:

- 2.1 To lay down policy framework for abiding by the Know Your Customer Norms and Anti-Money Laundering Measure as set out by Reserve Bank of India, based on the recommendations of the Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.
- 2.2 To enable the Bank to know/ understand the customers and their financial dealings better, thereby helping all concerns to manage KYC-AML-CFT related risks prudently.
- 2.3 To prevent the Bank from being used intentionally or unintentionally by criminal elements for money laundering or terrorist financing activities.
- 2.4 To put a proper control mechanism for detecting and reporting suspicious transactions under the statutory and regulatory provisions.
- 2.5 To ensure that all the provisions of Prevention of Money-laundering Act, 2002 and the Rules made thereunder and all subsequent amendments to it are duly complied with and
- 2.6 To ensure compliance with guidelines/instructions issued by the regulators, including FIU-IND and RBI.

- 2.7 To consider adoption of best international practices taking into account FATF standards and FATF guidance notes, for managing risks better.
- 2.8 To take necessary steps to ensure that the relevant staff are adequately trained in KYC / AML procedures.
- 2.9 The Board approved policy on KYC / AML / CFT is subject to annual review

### 3. **Applicability**

- 3.1 RBI Master Direction – Know Your Customer (KYC) Direction, 2016 dated February 25, 2016, and updated as of January 04, 2024, on adoption by our Bank, apply to our Bank being the entity regulated by RBI.
- 3.2 The provisions of KYC Policy guidelines shall apply to all the branches and offices of the Bank.

### 4. **Definitions**

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

- 4.1 (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:
- 4.1.1 "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.

4.1.2 "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 to it.

4.1.3 "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.

4.1.4 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 this sub-clause-

1. "Controlling ownership interest" means ownership of / entitlement to more than 10 percent of the company's shares or capital or profits.

2. "Control" shall include the right to appoint the majority of the directors or 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 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-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: The 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 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.

e. Where no natural person is identified under (a), (b), (c) or (d) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

4.1.5 “Certified Copy of OVD” - Obtaining a certified copy by the bank shall mean comparing the copy of the officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Bank

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

- Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
- Branches of overseas banks with whom Indian banks have relationships,
- Banker Abroad.
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

4.1.6 "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 the digital form of a customer.

4.1.7 "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 and shall include:

The Managing Director or a whole-time Director, duly authorized by the Board of Directors of the Bank, being a company.

4.1.8 "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 an authorised officer of the Bank is taking such live photo as per the provisions contained in the Act.

4.1.9 "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.]

4.1.10 "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 how the issuer uses the Digital locker System.)

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

4.1.12 "Non-profit organisations" (NPO) means any entity or organization constituted for religious or charitable purposes as referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961). These entities should be registered as a trust or a society under the Societies Registration Act, 1860, or any similar State legislation or as a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

4.1.13 The "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 the 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 an 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 licence agreements with such employers allotting official accommodation;
  - a. The customer shall submit OVD with the current address within three months of submitting the documents specified at 'b' above, failing which the operations in the account shall be restricted (Debit-freeze).
  - b. 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 letters 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 after its issuance, provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

4.1.14 “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).

#### 4.1.15 Proof of possession of Aadhaar Number

The Aadhaar holder can use any of the following documents to prove possession of the Aadhaar number subject to the Bank’s right to verify the genuineness of the mentioned document. The delivery of Aadhaar in any of its forms may not be considered satisfactory proof of possession of the Aadhaar number. The Aadhaar number holder may have to provide additional documents as may be required by the Bank.

- a. Aadhaar letter: Issued by the Authority carries the name, address, gender, photo and date of birth details of the Aadhaar card 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. The Authority digitally signs this as per the Information Technology Act (Act Number 21 of 2000), which provides legal recognition of electronic records with the 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. The Authority digitally signs this as per the Information Technology Act (Act Number 21 of 2000), which provides legal recognition of electronic records with the digital signature.

- d. Aadhaar Paperless Offline e-KYC: An XML document generated by the Authority containing name, address, gender, photo and the date of birth details of the Aadhaar number holder. The Authority digitally signs this as per the Information Technology Act (Act Number 21 of 2000), which provides legal recognition of electronic records with the digital signature.

4.1.16 "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).

4.1.17 "Principal Officer" means an officer at the management level nominated by the Bank, responsible for furnishing information as per rule 8 of the PMLA Rules.

4.1.18 "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 not to have an economic rationale or bonafide 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 transactions involving funds suspected to be linked or associated 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.

4.1.19 A 'Small Account' means a savings account that 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 12.10.

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

- opening of an account;
- 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;
- the use of a safety deposit box or any other form of safe deposit;
- entering into any fiduciary relationship;

- any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- establishing or creating a legal person or legal arrangement.

4.1.21 "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 their UCIC.

4.1.22 "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, informed-consent based audio-visual interaction with the customer 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 an audit trail of the process. Such process shall be treated as face to face process for the purpose of this KYC Policy.

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

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

4.2.2 "Customer" means a person 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.

- 4.2.3 "Walk-in Customer" means a person who does not have an account-based relationship with the Bank but undertakes transactions with the Bank.
- 4.2.4 "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.
- 4.2.5 "Customer identification" means undertaking the process of CDD.
- 4.2.6 "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.
- 4.2.7 "IGA" means Inter-Governmental Agreement between India and the USA to improve international tax compliance and implement FATCA of the USA.
- 4.2.8 "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR for individuals and legal entities.
- 4.2.9 "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank.
- 4.2.10 "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.

4.2.11 "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

4.2.12 "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/ Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

4.2.13 "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.

4.2.14 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 a number of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

4.3 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 and regulations made



thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

**5. The KYC policy includes the following four key elements:**

- A. Customer Acceptance Policy
- B. Risk Management.
- C. Customer Identification Procedures (CIP) and
- D. Monitoring of Transactions

**6. Money Laundering and Terrorist Financing Risk Assessment by Bank**

- 6.1 Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

**7. Compliance with KYC policy:**

Bank to ensure compliance with KYC Policy through:

- 7.1 Allocation of responsibility through SOP/ Circulars for effective implementation of policies and procedures at HO/ Regional Office level.
- 7.2 All HO Departments to ensure compliance of KYC guidelines in their respective areas of operation, products, services, and activities.
- 7.3 Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements is done by Compliance Department, HO.

- 7.4 Concurrent / internal audit system to verify the compliance with KYC/ AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.
- 7.5 Concurrent/ internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports from CBS.
- 7.6 Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
- 7.7 PML Rules require all offices of the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels.

The risk assessment should-

- a. be documented;
- b. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
- c. be kept up to date; and
- d. be available to competent authorities and self-regulating bodies.

The implementation of KYC-AML guidelines by branches in letter and spirit has to be ensured by Regional Heads and the same is to be checked during their visit to branches.

## **8. Customer Acceptance Policy (CAP)**

The following provisions shall form the Customer Acceptance Policy:

- 8.1 No account shall be opened in anonymous or fictitious/ benami names.
- 8.2 Accounts shall not be opened if the bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/ information provided. If necessary, the Bank shall consider filing an STR in cases where the relevant CDD measures concerning the customer are not complied.
- 8.3 All transactions or account-based relationships shall be undertaken only after following the CDD procedure.
- 8.4 The mandatory information required for KYC purposes during the account opening process and periodic updates shall be specified.
- 8.5 Additional information not specified in our internal KYC Policy may be obtained with the explicit consent of the customer.
- 8.6 CDD procedures shall be applied at the Unique Customer Identification Code (UCIC) level. Therefore, if an existing KYC compliant customer of our bank wishes to open another account, a fresh CDD exercise shall not be necessary.
- 8.7 CDD procedures shall be followed for all joint account holders during the account opening process.
- 8.8 The circumstances under which a customer is permitted to act on behalf of another person/ entity shall be clearly defined.
- 8.9 Suitable systems shall be implemented to ensure that the identity of the customer does not match with any person or entity listed in the sanctions lists indicated in Section 27 of the KYC Policy.

8.10 When obtaining a Permanent Account Number (PAN), the same shall be verified using the verification facility provided by the issuing authority.

8.11 In cases where an equivalent e-document is obtained from the customer, our bank shall verify the digital signature in accordance with the provisions of the Information Technology Act, 2000 (21 of 2000).

8.12 If Goods and Services Tax (GST) details are available, the GST number shall be verified using the search/ verification facility provided by the issuing authority.

**Ensuring Access to Banking/ Financial Facilities:**

8.13 Our Customer Acceptance Policy shall not result in the denial of banking or financial facilities to members of the general public, especially those who are financially or socially disadvantaged.

**Reporting Suspicion of Money Laundering or Terrorist Financing:**

8.14 If our bank forms a suspicion of money laundering or terrorist financing and reasonably believes that conducting the CDD process will alert the customer, we shall not pursue the CDD process. Instead, we will file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit - India (FIU-IND).

**9. Risk Perception in respect of Customer:**

9.1 "Customer Risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by the customer.

9.2 For categorizing a customer as Low Risk, Medium Risk and High Risk, the parameters considered are customer's identity, social/ financial status, nature of business activity, information about the client's business and their location 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.

9.2.1 Low Risk Customers (Level 1 customers):

Individuals (other than High Net worth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as Low Risk customers.

9.2.2 Medium Risk Customers (Level 2 customers):

Customers who are likely to pose a higher than average risk to the Bank should be categorised as medium or high risk. For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her client profile, etc. besides proper identification.

9.2.3 High Risk Customers (Level 3 customers):

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank shall subject such accounts to enhanced monitoring on an ongoing basis.

## 10. Customer Identification Procedure (CIP)

Customer identification Procedure means undertaking the process of CDD (Customer Due Diligence i.e. Identifying and verifying the customer and the beneficial owner).

10.1 Bank shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of banking relationship. The Bank shall observe due diligence based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).

10.2 Bank shall have a policy approved by the Board which clearly spells out the Customer Identification Procedure to be carried out at different stages, i.e.,

- a) While establishing a banking relationship;
- b) While carrying out a financial transaction;
- c) Carrying out any international money transfer operations for a person who is not an account holder of the bank.
- d) When the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;
- e) When bank sells third party products as agent;
- f) While selling Bank's own products, payment of dues of credit cards/ sale and reloading of prepaid/ travel cards and any other product for more than Rs. 50,000/-.
- g) When carrying out transactions for a non-account based customer, that is a walk-in-customer, where the amount is equal to or exceeds Rs. 50,000/-,

whether conducted as a single transaction or several transactions that appear to be connected;

- h) When the 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 Rs. 50,000/-.
- i) Bank shall ensure that introduction is not to be sought while opening accounts.

‘Mandatory’ information required for KYC purpose which the customer is obliged to give while opening an account should be obtained at the time of opening the account/ during periodic updation.

## **11. Customer Due Diligence requirements while opening accounts**

11.1 Customer Due Diligence (CDD) Procedure and sharing KYC information with Central KYC Records Registry (CKYCR): Branches shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for ‘individuals’ and ‘Legal Entities’ as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

### **11.2 Accounts of individuals:**

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

a. The Aadhaar number where:

- The individual 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
- The individual decides to submit their Aadhaar number voluntarily to the Bank or any other entity notified under the first proviso to sub-section (1) of section 11A of the Prevention of Money Laundering Act (PML Act); or

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

(ab) The proof of possession of Aadhaar number where offline verification cannot be carried out or any Officially Valid Document (OVD) or the equivalent electronic document thereof containing the details of their identity and address; or

(ac) The KYC Identifier with an explicit consent to download records from the Central KYC Registry (CKYCR); and

b. The Permanent Account Number (PAN) or the equivalent electronic document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

c. Such other documents including those related to the nature of business and financial status of the customer or the equivalent electronic documents thereof as may be required by the Bank.

d. A recent Passport size photograph.

Provided that where the customer has submitted:

- i. Aadhaar number under clause (a) above to the Bank or to any entity notified under the first proviso to sub-section (1) of section 11A of the PML Act, the Bank shall carry out authentication of the customer's Aadhaar number using the e-KYC authentication facility provided by the Unique Identification Authority of India. Furthermore, if the customer wants to provide a current address different from the address as per the



identity information available in the Central Identities Data Repository, they may give a self-declaration to that effect to the Bank.

- ii. Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.
- iii. An equivalent electronic 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 Digital KYC Process.
- 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 Digital KYC Process.
- v. KYC Identifier under clause (ac) above, the Bank shall retrieve the KYC records online from the CKYCR in accordance with Section 29.11.

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 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 electronic document is not submitted.

Provided further that in case 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, the Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent electronic 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 7. The Bank shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds for granting exceptions, 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: The Bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out their Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric-based e-KYC authentication can be done by bank officials, business correspondents, or 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, 2016, and the regulations made thereunder.

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

11.3.1 There must be a specific consent from the customer for authentication through OTP.

11.3.2 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.

11.3.3 The aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees 2 Lakh.

11.3.4 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.

11.3.5 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 12 is carried out. If Aadhaar details are used under Section 12, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

11.3.6 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.

11.3.7 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 nonface- 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.

11.3.8 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.

#### 11.4 Video-based Customer Identification Process (V-CIP)

The Bank may undertake 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, the Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 16, 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 14.
- iii. Updation/ Periodic updation of KYC for eligible customers.

The Bank shall adhere to the following minimum standards:

- a. V-CIP Infrastructure:
  - i. Our bank has complied with the RBI guidelines on the minimum baseline cybersecurity and resilience framework for banks, as well as general guidelines on IT risks. Our technology infrastructure is housed within our own premises, and the V-CIP connection and interaction originate from our secure network domain. Any technology-related outsourcing for the process complies with relevant RBI guidelines.
  - ii. We ensure end-to-end encryption of data between the customer's device and the hosting point of the V-CIP application, adhering to appropriate encryption standards. Customer consent is recorded in an auditable and alteration-proof manner.
  - iii. Our V-CIP infrastructure/ application prevents connections from IP addresses outside India or spoofed IP addresses.
  - iv. The video recordings captured during V-CIP include live GPS coordinates (geo-tagging) of the customer and date-time stamp. The video quality is adequate to allow clear identification of the customer.
  - v. Our V-CIP application incorporates face liveness/ spoof detection and face matching technology with a high degree of accuracy. We leverage appropriate artificial intelligence (AI) technology to ensure the robustness of V-CIP.
  - vi. We regularly upgrade our technology infrastructure, including application software and workflows, based on experience with detected/ attempted/ forged identity cases. Any detected case of forged identity through V-CIP is reported as a cyber event under the existing regulatory guidelines.
  - vii. Our V-CIP infrastructure undergoes necessary tests, including Vulnerability Assessment, Penetration Testing, and a Security Audit, to ensure robustness and end-

to-end encryption capabilities. These tests are conducted by empanelled auditors of the Indian Computer Emergency Response Team (CERT-In) and are carried out periodically in conformance with internal/ regulatory guidelines.

- viii. The V-CIP application software and relevant APIs/ webservice undergo appropriate testing for functionality, performance, and maintenance strength before being used in a live environment. Only after closing any critical gaps identified during such tests, the application is rolled out. These tests are also carried out periodically in conformity with internal/ regulatory guidelines.

#### 11.5 V-CIP Procedure:

- i. We have formulated a clear workflow and standard operating procedure for V-CIP, which is adhered to by our officials specially trained for this purpose. Our officials are capable of conducting liveness checks, detecting fraudulent manipulation, and identifying suspicious conduct of the customer.
- ii. Disruption of any sort, such as pausing of video or call reconnection, does not result in the creation of multiple video files. In case of call drop/ disconnection, a fresh session is initiated.
- iii. The sequence and/ or type of questions during video interactions are varied to establish real-time interactions and prevent pre-recorded interactions.
- iv. Any prompting observed at the end of the customer results in the rejection of the account opening process.
- v. We consider whether the V-CIP customer is an existing or new customer, or if it relates to a case previously rejected or if the name appears in any negative list at an appropriate stage of the workflow.
- vi. Our authorized officials performing V-CIP record audio-video, capture photographs of the customer for identification purposes, and obtain identification information using any of the following methods:
  - (i) OTP-based Aadhaar e-KYC authentication
  - (ii) Offline verification of Aadhaar for identification
  - (iii) Downloading KYC records from CKYCR using the KYC identifier provided by the customer
  - (iv) Equivalent e-document of Officially Valid Documents (OVDs), including documents issued through DigiLocker

It is ensured that the Aadhaar number is redacted or blacked out in accordance with Section 12.

- vii. In cases of offline verification of Aadhaar using an XML file or Aadhaar Secure QR Code, we ensure that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.
- viii. Following the prescribed period of three days for using Aadhaar XML file/ Aadhaar QR code, we ensure that the V-CIP video process is completed within three working days of downloading/ obtaining identification information through CKYCR/ Aadhaar authentication/ equivalent e-document, if, in rare cases, the entire process cannot be completed at one go or seamlessly. However, we take measures to ensure that no incremental risk is added due to this.
- ix. If the customer's address differs from the one indicated in the OVD, we capture suitable records of the current address as per existing requirements. We also confirm the economic and financial profile/ information submitted by the customer during V-CIP in a suitable manner.
- x. We capture a clear image of the PAN card provided by the customer, except in cases where an e-PAN is provided. PAN details are verified from the database of the issuing authority, including through DigiLocker.
- xi. The use of a printed copy of an equivalent e-document, including e-PAN, is not valid for V-CIP.
- xii. The authorized official of our bank ensures that the customer's photograph in the Aadhaar/ OVD and PAN/ e-PAN matches the customer undertaking V-CIP, and the identification details in Aadhaar/ OVD and PAN/ e-PAN match the details provided by the customer.
- xiii. Assisted V-CIP is permissible when our bank takes the help of Business Correspondents (BCs) to facilitate the process at the customer end. We maintain the details of the BC assisting the customer, if BC services are utilized. However, the ultimate responsibility for customer due diligence lies with our bank.
- xiv. All accounts opened through V-CIP are subject to concurrent audit before becoming operational, ensuring the integrity of the process and the acceptability of the outcome.
- xv. We comply with all matters required under other statutes, such as the Information Technology (IT) Act, in addition to those specified in this policy.

#### 11.6 V-CIP Records and Data Management:

- i. All data and recordings of V-CIP are stored in systems located within India. We ensure that video recordings are stored safely and securely, with a date and time stamp for easy historical data search. The existing instructions on record management, as stipulated in this policy, also apply to V-CIP.

We preserve the activity log along with the credentials of the official performing V-CIP.

#### 11.7 Introduction of accounts:

11.7.1 Since introduction from an existing customer is not necessary for opening accounts under PML Act and Rules or the RBI's extant instructions, branches shall not insist on introduction for opening of bank accounts. After passing of PML Act and introduction of document based verification of identity/ address of the proposed account holders, the accounts opened with proper documents are considered as acting in good faith and without negligence by the banks.

#### 11.8 Accounts of married woman:

11.8.1 As per the amendment to the Rules, 2005 (Gazette notification dated 22.09.2015), a document shall be deemed to 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 a Gazette notification, indicating such a change of name.

11.8.2 Accordingly, Branches shall accept a copy of marriage certificate issued by the State Government or Gazette notification indicating change in name, together with a certified copy of the "Officially Valid Document" in the existing name of the person while

establishing an account-based relationship or while undergoing periodic updation exercise.

#### 11.9 Small Accounts:

11.9.1 Notwithstanding anything contained in Section 12 and as an alternative thereto, in case an individual who desires to open a bank account, banks 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.

11.9.2 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. The bank shall obtain a self-attested photograph 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. Banks shall ensure 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 for such 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 12.
- 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 12.

## **12. Basic Savings Bank Deposit Accounts**

- 12.1 As per RBI guidelines, the Basic Savings Bank Deposit Account should be considered a normal banking service available to all.
- 12.2 The Basic Savings Bank Deposit Account is subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time. If such account is opened on the basis of simplified KYC norms, the

account would additionally be treated as a “Small Account” and would be subject to conditions stipulated for small accounts.

12.3 In case the address mentioned as per “proof of address” undergoes a change, the document mentioned in point no 4.1.13 is to be obtained for limited period and the customer has to submit updated Officially Valid Document with current address within a period of three months of submitting the above document.

12.4 Branches are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the Bank to another branch. KYC once done by one branch of the Bank shall be valid for transfer of the account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customer shall be allowed to transfer his account from one branch to another branch without restrictions.

12.5 If an existing KYC compliant customer of the Bank desires to open another account in the Bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

12.6 For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the branch may rely on a third party; subject to the conditions that:

12.6.1 Records of the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

12.6.2 The branch takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

12.6.3 The branch is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;

12.6.4 The third party is not based in a country or jurisdiction assessed as high risk; And

12.6.5 The branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

### 13. **Account opened using OTP based e-KYC, in non-face-to-face mode**

This section of our KYC Policy outlines the specific conditions and requirements to ensure compliance with the guidelines regarding accounts opened using Aadhaar OTP-based e-KYC in non-face-to-face mode.

a. Customer Consent:

- i. Accounts opened using Aadhaar OTP based e-KYC require specific consent from the customer for authentication through OTP.

b. Mobile Number Verification and Change:

- i. As a risk-mitigating measure, our bank shall ensure that transaction alerts, OTPs, and other relevant communication are sent only to the mobile number registered with Aadhaar.
- ii. Our bank shall have a board-approved policy that establishes a robust process for due diligence when dealing with requests for changing the mobile number associated with such accounts.

c. Account Balance Limit:

- i. The aggregate balance of all deposit accounts for a customer shall not exceed rupees one lakh.

- ii. If the balance exceeds the specified threshold, the account shall cease to be operational until Customer Due Diligence (CDD) procedures mentioned at point (v) below are completed.
- d. Credit Limit:
  - i. The aggregate of all credits in a financial year, across all deposit accounts, shall not exceed rupees two lakh.
- e. Borrowal Accounts:
  - i. Only term loans shall be sanctioned for accounts opened using OTP based e-KYC.
  - ii. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- f. Account Validity and Identification:
  - i. Accounts, both deposit and borrowal, opened using OTP-based e-KYC shall not remain active for more than one year unless identification is carried out as per Section 12.
  - ii. If Aadhaar details are used under Section 12, the complete process, including fresh Aadhaar OTP authentication, shall be followed.
- g. Incomplete CDD Procedure:
  - i. If the CDD procedure mentioned above is not completed within one year for deposit accounts, the accounts shall be closed immediately.
  - ii. For borrowal accounts, no further debits shall be allowed if the CDD process is not completed within the specified timeframe.
- h. Declaration and CKYCR Upload:
  - i. A declaration shall be obtained from the customer stating that no other account has been opened or will be opened using OTP based KYC in non-face-to-face mode with any other regulated entity.

- ii. While uploading KYC information to Central KYC Registry (CKYCR), our bank shall clearly indicate that such accounts were opened using OTP based e-KYC, and other regulated entities shall not open accounts based on the KYC information of accounts opened with OTP-based e-KYC procedure in non-face-to-face mode.

- i. **Monitoring and Compliance:**

Our bank shall establish strict monitoring procedures, including systems to generate alerts in case of any non-compliance or violation, to ensure adherence to the above-mentioned conditions.

#### **14. Accounts of Foreign students studying in India:**

Considering that foreign student arriving in India are facing difficulties in complying with the Know Your Customer (KYC) norms while opening a bank account due to nonavailability of any proof of local address, the following procedure shall be followed for opening accounts of foreign students who are not able to provide an immediate address proof while approaching the Bank for opening bank account: -

14.1.1 Branches may 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.

14.1.2 Branches should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.

14.1.3 During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.

14.1.4 The account would be treated as a normal NRO account after verification of address and will be operated in terms of existing guidelines issued in the Manual of instructions on Non-Resident Deposits and Circulars issued from time to time.

14.1.5 Students with Pakistani nationality will need prior approval of the Reserve Bank of India for opening the account.

## **15. Accounts of Politically Exposed Persons (PEPs) resident outside India**

15.1.1 Bank shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. Branches shall maintain a database of PEP accounts in the Branch. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

15.1.2 The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming a Politically Exposed Person (PEP), has to be taken by the respective Regional Office

15.1.3 In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where a PEP is the ultimate beneficial owner shall be categorized as 'High Risk' so that appropriate transaction alerts are generated and the accounts are subjected to enhanced CDD on an ongoing basis.

15.1.4 Bank shall have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

**16. Accounts of persons other than individuals:**

16.1 Bank need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Bank shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

**17. CDD Measures for Sole Proprietary firms**

For opening an account in the name of a sole proprietary firm, our bank shall carry out Customer Due Diligence (CDD) of the individual (proprietor) as per the guidelines set by the Reserve Bank of India (RBI).

a. Proof of Business/ Activity:

In addition to the CDD of the proprietor, our bank shall obtain any two of the following documents or their equivalent e-documents as proof of business/ activity in the name of the proprietary firm:

- i. Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
- ii. Certificate/ license issued by the municipal authorities under the 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 or license/ 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, landline telephone bills, etc.

b. Discretionary Acceptance:

In cases where our bank determines that it is not feasible for the customer to furnish two of the aforementioned documents, we may, at our discretion, accept only one such document as proof of business/ activity. However, in such instances, we shall undertake contact point verification and collect additional information and clarification to establish the existence of the firm. We shall confirm and satisfy ourselves that the business activity has been verified from the address of the proprietary concern.

## 18. CDD Measures for Legal Entities

- a. For opening an account of a company, our Bank shall obtain certified copies or equivalent e-documents of the following documents:



- i. Certificate of incorporation
- ii. Memorandum and Articles of Association
- iii. Permanent Account Number (PAN) of the company
- iv. Resolution from the Board of Directors and power of attorney granted to its managers, officers, or employees to transact on its behalf
- v. Documents specified in Section 12 pertaining to the beneficial owner, managers, officers, or employees holding an attorney to transact on the company's behalf
- vi. Names of relevant persons holding senior management positions
- vii. Registered office and principal place of business, if different
- b. For opening an account of a partnership firm, our Bank shall obtain certified copies or equivalent e-documents of the following documents:
  - i. Registration certificate
  - ii. Partnership deed
  - iii. Permanent Account Number (PAN) of the partnership firm
  - iv. Documents specified in Section 12 pertaining to the beneficial owner, managers, officers, or employees holding an attorney to transact on its behalf
  - v. Names of all the partners
  - vi. Address of the registered office and principal place of business, if different
- c. For opening an account of a trust, our Bank shall obtain certified copies or equivalent e-documents of the following documents:
  - i. Registration certificate
  - ii. Trust deed
  - iii. Permanent Account Number (PAN) or Form No. 60 of the trust
  - iv. Documents specified in Section 12 pertaining to the beneficial owner, managers, officers, or employees holding an attorney to transact on its behalf

- v. Names of beneficiaries, trustees, settlor, protector, if any and authors of the trust
- vi. Address of the registered office of the trust
- vii. List of trustees and documents specified in Section 12 for those discharging the role as trustee and authorized to transact on behalf of the trust
- d. For opening an account of an unincorporated association or a body of individuals, our Bank shall obtain certified copies or equivalent e-documents of the following:
  - i. Resolution of the managing body of the association or body of individuals
  - ii. Permanent Account Number (PAN) or Form No. 60 of the unincorporated association or body of individuals
  - iii. Power of attorney granted to transact on its behalf
  - iv. Documents specified in Section 12 pertaining to the beneficial owner, managers, officers, or employees holding an attorney to transact on its behalf
  - v. Information required 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'. The term 'body of individuals' includes societies.

- e. For opening an account of a customer who is a juridical person (not specifically covered earlier) such as societies, universities, local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, our Bank shall obtain and verify certified copies or equivalent e-documents of the following:
  - i. Document showing the name of the person authorized to act on behalf of the entity
  - ii. Documents specified in Section 12 of the person holding an attorney to transact on its behalf
  - iii. Documents required to establish the legal existence of such an entity/ juridical person

Provided that in case of a trust, the Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (c), (g) and (h) of Section 11.2 of this policy.

- f. For opening an account of a Hindu Undivided Family, our Bank shall obtain certified copies of the following documents:
  - i. Identification information as mentioned under Section 12 in respect of the Karta and Major Coparceners
  - ii. Address documents, as specified in Section 12
  - iii. Declaration of HUF and its Karta
  - iv. Recent passport photographs duly self-attested by major coparceners along with their names and addresses

Permanent Account Number (PAN) or equivalent e-document thereof, or Form No. 60 as defined in Income-tax Rules, 1962.

#### **19. Identification of Beneficial Owner**

For opening an account of a Legal Person who is not a natural person, our Bank shall undertake the identification of the beneficial owner(s) and ensure all reasonable steps are taken to verify their identity, in accordance with the provisions specified in sub-rule (3) of Rule 9 of PML (Maintenance of Records) Rules 2005. The following considerations shall be taken into account:

- a. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) a subsidiary of such listed entities; it shall not be 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, where the customer is acting on behalf of another person as trustee/ nominee or any other intermediary, our Bank shall determine the nature of the arrangement. In such cases, we shall obtain satisfactory

evidence of the identity of the intermediaries and the individuals on whose behalf they are acting, as well as details regarding the nature of the trust or other arrangements in place.

## 20. **On-going Due Diligence**

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

20.2 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.

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

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

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

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

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.

## 21. Periodic updation of KYC

### a. Risk-Based Approach for Periodic Updation:

The Bank shall adopt a risk-based approach for the periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. The frequency of periodic updation shall be as follows:

- i. High-risk customers: At least once every two years from the date of account opening or the last KYC updation.
- ii. Medium-risk customers: At least once every eight years from the date of account opening or the last KYC updation.
- iii. Low-risk customers: At least once every ten years from the date of account opening or the last KYC updation.

### b. Individuals:

#### a. No Change in KYC Information:

In cases where there is no change in the KYC information, we shall obtain a self-declaration from the customer through their registered email ID, registered mobile number, ATMs, digital channels (such as online banking, mobile application), letter, etc.

#### b. Change in Address:

If there is a change only in the address details of the customer, we shall obtain a self-declaration of the new address through the customer's registered email ID, registered mobile number, ATMs, digital channels, letter, etc. The declared address shall be verified through positive confirmation within two months using methods such as address verification letter, contact point verification, deliverables, etc.

Additionally, we may choose to obtain a copy of Officially Valid Document (OVD) or deemed OVD or equivalent e-documents as proof of address declared by the customer. The requirement of obtaining additional address proof shall be clearly specified in our internal KYC policy.

c. Accounts of Customers Becoming Major:

For customers who were minors at the time of account opening, we shall obtain fresh photographs upon their reaching adulthood. At that time, we shall ensure that the current Customer Due Diligence (CDD) documents are available. If necessary, fresh KYC may be carried out for such customers.

d. Aadhaar OTP-based e-KYC for Periodic Updation:

Aadhaar OTP-based e-KYC in a non-face-to-face mode may be used for periodic updation. The conditions specified in Section 17 are not applicable for KYC updation through Aadhaar OTP-based e-KYC in a non-face-to-face mode.

e. Declaration of Current Address:

If the current address is different from the address in Aadhaar, positive confirmation is not required. However, we shall ensure that the mobile number for Aadhaar authentication is the same as the one available in the customer's profile to prevent any fraud.

c. Customers other than Individuals:

i. No Change in KYC Information:

In case there is no change in the KYC information of a Legal Entity (LE) customer, we shall obtain a self-declaration in this regard through the LE's email ID, ATMs, digital channels, letter from an authorized official of the LE, board resolution, etc. Additionally, we shall ensure that the Beneficial Ownership (BO) information is accurate and update it if required.

ii. Change in KYC Information:

In case of a change in KYC information, we shall undertake the KYC process equivalent to onboarding a new LE customer.

**Additional Measures:**

In addition to the above, we shall ensure the following:

The KYC documents of the customer as per the current CDD standards are available. Even if there is no change in customer information, if the documents available do not meet the current CDD standards or if the validity has expired, we shall undertake the KYC process equivalent to onboarding a new customer.

PAN details, if available, shall be verified from the database of the issuing authority during periodic KYC updation.

We shall provide an acknowledgment to the customer mentioning the date of receipt of relevant documents, including self-declarations, for carrying out periodic updation. The obtained information/ documents shall be promptly updated in our records/ database, and an intimation regarding the date of KYC updation shall be provided to the customer.

We may consider offering the facility of periodic updation of KYC at any branch for customer convenience, as specified in our internal KYC policy.

A risk-based approach shall be adopted, and any additional measures not mandated under the above instructions shall be clearly specified in our internal KYC policy, duly approved by the Board of Directors or any delegated committee.

**d. Submission of Updated Documents:**

Customers shall submit updates to us within 30 days of any changes in the documents submitted at the time of establishing the business relationship/ account-based relationship.

**e. Ceasing Operations and Account Closure:**

For customers who fail to submit their Permanent Account Number (PAN) or equivalent e-document or Form No. 60, we shall temporarily cease operations in the account. Before temporarily ceasing operations, we shall provide accessible notice and a reasonable opportunity to be heard. In cases where customers explicitly state in writing that they do not want to submit their PAN or equivalent document, we shall close the account after establishing the customer's identity by obtaining applicable identification documents.

## 22. Miscellaneous

### 21.1 Operation of Bank Accounts & Money Mules

22.1.1 Money Mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering. “Money Mules” can be 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 to act as “money mules.” In order to minimize the operations of such mule accounts, Branches should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

22.1.2 If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

### 22.2 Simplified norms for Self Help Groups (SHGs):

22.2.1 In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening Savings Bank accounts and credit linking of their accounts, following simplified norms shall be followed by branches:

22.2.2 KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.

22.2.3 Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.



### 22.3 Walk-in Customers

22.3.1 In case of transactions carried out by a non-account based customer, i.e., a walk-in customer, where the amount of transaction is equal to or exceeds Rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address shall be verified.

22.3.2 If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/-the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND. The identity and address of the Walk-in customer shall be verified by obtaining KYC documents and records are to be maintained/ updated in the system. Bank shall also verify the identity of the customers for all international money transfer operations.

### 23. **Issue of Demand Drafts, etc., for more than Rs. 50,000/-**

23.1 Any remittance of funds by way of Demand Draft or any other mode and issue of Traveller's cheques for value of Rs. 50,000/- and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

23.2 Bank shall not make payment of cheques/ drafts/ pay orders/ banker's cheques if they are presented beyond the period of three months from the date of such instrument.

23.3 The name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheques etc by the issuing Bank with effect from 15th September 2018.

**24. Unique Customer Identification Code**

24.1 A Unique Customer Identification Code (UCIC) will help the Bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Bank to have a better approach to risk profiling of customers.

24.2 Branches/Operations team are required to strictly avoid creating multiple customer IDs while opening new accounts and in case of existing multiple IDs, branches have to carry out the process of de-duplication.

**25. Monitoring of Transactions:**

25.1 Ongoing monitoring is an essential element of effective KYC/ AML procedures. Branches should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

25.1.1 The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

25.2 Branches should pay particular attention to the following types of transactions:

25.2.1 Large and complex transactions including RTGS transaction, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

25.2.2 Transactions which exceed the thresholds prescribed for specific categories of accounts.

25.2.3 Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

25.2.4 High account turnover inconsistent with the size of the balance maintained.

25.3 Bank shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months.

25.4 Branches should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Branches should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the branches and in case they find such unusual operations in their accounts, the matter should be immediately reported to AML/CFT Centralized Unit for onward reporting to Reserve Bank and other appropriate authorities such as FIU-IND.

25.5 Supervisors should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt, necessary enquiries should be made with the account holders.

25.6 While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.

- 25.7 Branches are advised to mandatorily obtain either PAN or Form 60 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs. 50,000/- and above. If the customer appears to be structuring the transactions into a series of transactions below the threshold of Rs. 50,000/-, branches are required to obtain PAN or Form 60 (if PAN is not available) from the customer.
- 25.8 Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of obtention of PAN or Form 60, wherever the aggregate amount of transactions is Rs. 50,000/- and above.
- 25.9 All the staff members are instructed to maintain the standards of good conduct and behaviour expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

**26. Risk Management:**

- 26.1 The inadequacy or absence of KYC standards can subject the Bank to serious customer and counter party risks especially reputational, operational, legal and concentration risks. Reputational Risk is defined as “the potential that adverse publicity regarding the Bank’s business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution”. Operational Risk can be defined as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events”. Legal Risk is “the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank”. Concentration Risk although

mostly applicable on the assets side of the balance sheet, may affect the liabilities side as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the Bank's liquidity. It is worth noting that all these risks are interrelated. Any one of them can result in significant financial cost to the Bank as well as the need to divert considerable management time and energy to resolve problems that arise.

26.2 Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, operational and legal risk arising from such accounts, Bank shall aggregate and monitor significant balances and activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

26.3 Branches should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds. The Board of Directors of the Bank shall ensure that an effective KYC/AML/CFT programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters.

26.4 In addition, the following also to be ensured for effectively implementing the AML/CFT requirements:

26.4.1 Using a risk-based approach to address management and mitigation of various AML/ CFT risks.

26.4.2 Allocation of responsibility for effective implementation of policies and procedures.

26.4.3 Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.

26.4.4 Concurrent/internal audit/snap audit to verify the compliance with KYC/ AML policies and procedures.

26.4.5 Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals and to Board of Directors at monthly intervals by KYC Cell and AML/ CFT Centralised Unit.

26.4.6 Branches shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank.

26.4.7 Branches shall categorise the customers into low, medium and high-risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The Bank shall have a Board approved policy for risk categorisation and ensure that the same is meticulously complied with, to effectively help in

combating money laundering activities. The nature and extent of due diligence, shall be based on the following principles:

26.4.8 Bank has adopted a risk categorization model as advised by the Indian Banks Association.

26.5 The roles and responsibilities of various Wings and Sections with regard to KYC/AML/CFT matters are as follows:

26.5.1 Business development and Planning Section-

26.5.2 Issuance of guidelines pertaining to KYC/ AML/ CFT for Domestic deposits and implementation/monitoring of the same.

26.5.3 AML/ CFT Centralised Unit

26.5.4 Verification of implementation of KYC/ AML/ CFT guidelines including liaison with RBI/ IBA/ FIU/ other agencies, reporting to regulatory authorities and attending to STR, CTR, NTR, CBWTR and CCR alerts.

26.5.5 The Bank shall take steps to identify and assess the Money Laundering /Terrorism Financing risk for customers, as also for products/ services/ transactions/ delivery channels. Bank shall have controls and procedures in place to effectively manage and mitigate the risk adopting a risk-based approach. As a corollary, Bank shall adopt enhanced measures for products, services and customers with a medium or high risk rating.

26.6 CORRESPONDENT BANKING AND SHELL BANK:

## Correspondent Banking

Correspondent banking relationships play a vital role in facilitating cross-border transactions for our bank. In line with the recent regulatory amendments issued by the Reserve Bank of India (RBI), this section of our KYC Policy outlines the specific requirements and conditions for approving and maintaining cross-border correspondent banking relationships.

### a. Approval and Due Diligence:

- i. Banks shall establish a policy, approved by their Boards or a committee headed by the Chairman/ CEO/ MD, that sets parameters for approving cross-border correspondent banking relationships.
- ii. In addition to conducting normal Customer Due Diligence (CDD) measures, the following conditions shall apply to correspondent banking relationships:

Sufficient information about the nature of the respondent bank's business, including details of management, major business activities, level of Anti-Money Laundering/ Counter Financing of Terrorism (AML/ CFT) controls, purpose of opening the account, and identity of any third-party entities using correspondent banking services, shall be gathered.

Information regarding the regulatory/ supervisory framework in the respondent bank's home country and publicly available information about the institution's reputation and quality of supervision, including any history of ML/ TF investigations or regulatory actions, shall be considered.

- iii. The Bank 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.
- iv. 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.



- v. Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. Post facto approval from the Board or the designated committee shall also be sought.

b. Documentation and Responsibilities:

- i. The Bank shall clearly document and understand the respective AML/ CFT responsibilities of institutions involved.
- ii. The responsibilities of each bank with whom a correspondent banking relationship is established shall be clearly documented and understood.
- iii. For payable-through-accounts, the correspondent bank shall ensure that the respondent bank has conducted CDD on customers who have direct access to the accounts of the correspondent bank and is continuously performing due diligence on them.
- iv. The correspondent bank shall ensure that the respondent bank can promptly provide the relevant CDD information upon request.

c. Prohibited Practices:

- i. Correspondent relationships shall not be established with shell banks.
- ii. Correspondent banks shall not permit their accounts to be used by shell banks.
- iii. Banks shall exercise caution when establishing correspondent banking relationships with banks located in jurisdictions that have strategic deficiencies or have not made sufficient progress in implementing the Financial Action Task Force (FATF) Recommendations.

d. KYC/ AML Requirements:

- i. Banks shall ensure that respondent banks have robust KYC/ AML policies and procedures in place.

Enhanced due diligence procedures shall be applied for transactions conducted through correspondent accounts.

## 26.7 WIRE TRANSFERS:

### Wire Transfer Information Requirements

- A. Information requirements for wire transfers for the purpose of this KYC policy:
- i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information, including:
    - a. Name of the originator
    - b. Originator account number (if applicable)
    - c. Originator's address, national identity number, customer identification number, or date and place of birth
    - d. Name of the beneficiary
    - e. Beneficiary account number (if applicable)

In the absence of an account, a unique transaction reference number should be included, which permits the 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, the individual transfers are exempted from the requirements of clause (i) above in respect of originator information. However, they must include the originator's account number or unique transaction reference number, as mentioned above, and the batch file must contain 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 our bank (RE), shall be accompanied by the 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 our bank (RE), shall also be accompanied by the 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. Our bank (RE) shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial 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 our bank (RE) to comply with applicable reporting requirements under the PML Act, 2002, and the Rules made thereunder or any other statutory requirement in force.

#### B. Responsibilities of Ordering RE, Intermediary RE, and Beneficiary RE

- i. Ordering RE (Our Bank):

As the ordering RE, our bank shall ensure that all cross-border and qualifying domestic wire transfers (i.e., transactions as per clauses (iii) and (iv) of paragraph 'A' above) contain the required and accurate originator information and beneficiary information, as indicated.

Customer identification shall be conducted if a customer, who is not an account holder of our bank, intentionally structures 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 their identity. If the same transaction is found to be suspicious, a Suspicious Transaction Report (STR) may be filed with FIU-IND in accordance with the PML Rules.

Our bank shall not execute the wire transfer if it is unable to comply with the requirements stipulated in this section.

ii. Intermediary RE (Our Bank):

As the intermediary RE, our bank shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, our bank shall keep a record of all the information received from the ordering financial institution or another intermediary RE for a minimum period of five years.

Our bank shall take reasonable measures, consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

We shall have effective risk-based policies and procedures in place to determine: (a) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information; and (b) the appropriate follow-up action, including seeking further information. If the transaction is found to be suspicious, reporting to FIU-IND shall be done in accordance with the PML Rules.

iii. Beneficiary RE (Our Bank):

As the beneficiary RE, our 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 (i.e., transactions as per clauses (iii) and (iv) of paragraph 'A' above) that lack required originator information or required beneficiary information.

We shall have effective risk-based policies and procedures in place to determine: (a) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information; and (b) the appropriate follow-up action, including seeking further information. If the transaction is found to be suspicious, reporting to FIU-IND shall be done in accordance with the PML Rules.

## **27. Record Management**

Our Bank acknowledges the importance of maintaining accurate and comprehensive records in accordance with the provisions of the Prevention of Money Laundering (PML) Act and Rules. To ensure compliance, the following steps shall be taken regarding the maintenance, preservation, and reporting of customer information:

- a. Our Bank shall maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for a minimum period of five years from the date of the transaction.
- b. Records pertaining to the identification of customers and their addresses obtained during the account opening process and throughout the business relationship shall be preserved for a minimum period of five years after the business relationship is terminated.
- c. Our Bank shall promptly and efficiently make identification records and transaction data available to the competent authorities upon their request.
- d. We shall introduce a system for maintaining proper records of transactions as prescribed under Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005).
- e. All necessary information regarding transactions prescribed under PML Rule 3 shall be maintained, allowing for the reconstruction of individual transactions. This

includes details such as the nature of the transactions, amount, currency, date of the transaction, and the parties involved.

- f. Our Bank shall develop a robust system for the proper maintenance and preservation of account information. This system will facilitate easy and quick retrieval of data whenever required by the competent authorities.
- g. Records of customer identity and address, as well as records of transactions referred to in Rule 3, shall be maintained in either 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 identification data, account files, business correspondence, and the results of any analysis undertaken.

In the case of customers who are non-profit organizations, our Bank shall ensure that their details are registered on the DARPAN Portal of NITI Aayog. If such registration has not been completed, our Bank shall take the necessary steps to register the details on the DARPAN Portal. The registration records shall be maintained 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.

## **28. Combating Financing of Terrorism (CFT)**

Requirements/ Obligations under International Agreements:

- a. Communications from International Agencies:

The bank shall ensure compliance with Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, and its amendments.

The bank shall not maintain accounts in the name of individuals/ entities appearing in the lists of individuals and entities suspected of having terrorist links, as approved and periodically circulated by the United Nations Security Council (UNSC).

The two lists to be referred to are:

- i. The "ISIL (Da'esh) & Al-Qaida Sanctions List," established and maintained pursuant to Security Council resolutions 1267/1989/2253. The list is available at [<https://scsanctions.un.org/ohz5jen-al-qaida.html>].

- ii. The "Taliban Sanctions List," established and maintained pursuant to Security Council resolution 1988 (2011). The list is available at [\[https://scsanctions.un.org/3pppl-en-taliban.htm\]](https://scsanctions.un.org/3pppl-en-taliban.htm).

The bank shall also refer to the lists 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 shall be verified on a daily basis, and any modifications, additions, deletions, or other changes shall be diligently considered for compliance.

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

- i. The bank shall report details of accounts resembling any individuals/ entities in the lists to the Financial Intelligence Unit - India (FIU-IND) and advise the Ministry of Home Affairs (MHA) as required by the UAPA notification dated February 2, 2021.
- ii. The bank shall strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 for freezing assets under Section 51A of the UAPA, 1967. Compliance with the Order issued by the Government shall be ensured, and the list of Nodal Officers for UAPA can be accessed on the MHA website.

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

- i. The bank shall meticulously comply 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," as laid down in the Order dated January 30, 2023, by the Ministry of Finance, Government of India.
- ii. The bank shall not carry out transactions if the particulars of an individual/ entity match those in the designated list.
- iii. The bank shall conduct checks, at the time of establishing a relationship with a customer and periodically, to verify whether individuals and entities in the designated list hold any funds, financial assets, or economic resources in the form of bank accounts, etc.

- iv. In case of a match, the bank shall immediately inform the transaction details, along with full particulars of the funds, financial assets, or economic resources involved, to the Central Nodal Officer (CNO) designated under Section 12A of the WMD Act, 2005. A copy of the communication shall also be sent to the State Nodal Officer and the RBI. The bank shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts mentioned above.
- v. The bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- vi. If there are concrete reasons to believe that a customer's funds or assets fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the bank shall prevent such individuals/ entities from conducting financial transactions. Immediate intimation shall be provided to the CNO via email, FAX, and post.
- vii. Upon receiving an order to freeze assets under Section 12A from the CNO, the bank shall take necessary actions to comply with the order without delay.
- viii. The bank shall observe the process of unfreezing funds, etc., as per paragraph 7 of the Order. Any application received from an individual/ entity regarding unfreezing shall be promptly forwarded, along with full details of the frozen asset provided by the applicant, to the CNO via email, FAX, and post, within two working days.
- ix. The Bank shall undertake 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.

d. Compliance with UNSCR 1718 Sanctions List:

The bank shall verify the "UNSCR 1718 Sanctions List of Designated Individuals and Entities" available at [<https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>] on a daily basis to consider any modifications, additions, deletions, or other changes. The bank shall 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.

e. Obligations under other UNSCRs and UAPA:

In addition to the above, the bank shall take into account other United Nations Security Council Resolutions (UNSCRs) and lists in the first schedule and the fourth schedule of the Unlawful Activities (Prevention) (UAPA) Act, 1967, and any amendments thereto for compliance with Government orders on the implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

f. Jurisdictions that do not or insufficiently apply the FATF Recommendations:

- i. The bank shall consider FATF Statements circulated by the Reserve Bank of India (RBI) and publicly available information to identify countries that do not or insufficiently apply the Financial Action Task Force (FATF) Recommendations. The Bank shall apply enhanced due diligence measures, 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.
- ii. 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: Legitimate trade and business transactions with countries and jurisdictions mentioned in the FATF statement are not precluded.

- i. The bank shall examine the background and purpose of transactions with persons from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Written findings, along with all supporting documents, shall be retained and made available to the Reserve Bank and other relevant authorities upon request.

g. Leveraging Technological Innovations for Name Screening:

The bank is encouraged to leverage the latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

## 29. Reporting Requirements

### 29.1 Reporting to Financial Intelligence Unit-India

29.1.1 In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by nonprofit organisations [NPO means any entity or organisation 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 (erstwhile Section 25 of Companies Act, 1956) Section 8 of the Companies Act, 2013], cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

29.1.2 The Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyaपुरi, New Delhi-110021. Website - <http://fiuindia.gov.in/>

29.1.3 FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website. FIU –INDIA in their REPORTING FORMAT

GUIDE, informed that for account based transaction, bank shall report in ACCOUNT BASED REPORTING FORAMT (ARF) and wherever transaction without account based relationship with the customer, bank shall report in TRANSACTION BASED REPORTING FORMAT (TRF).

29.1.4 While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Bank shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

The Bank 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.

29.1.5 As a part of transaction monitoring mechanism, Bank shall put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. The software shall be robust enough to throw the alerts for effective identification and reporting of suspicious transactions.

29.2 As per Rule 7 of PML Rules, the procedure and manner of furnishing information shall be as under:

29.2.1 The Bank shall communicate to the Director, FIU IND the name, designation and address of the Designated Director and the Principal Officer.

29.2.2 The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity (details of above clauses are furnished under para 6.1). A copy of such information shall be retained by the Principal Officer for the purposes of official record.

29.2.3 The Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in clauses (A),(B),(BA),(C),(D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by its Regulator.

29.2.4 The Bank, its Designated Director, officers and employees shall observe the procedure and the manner of furnishing information as specified by its Regulator.

### 30. **General Guidelines:**

#### 30.1 Confidentiality of customer information:

30.1.1 The information collected from the customer 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 etc. Information sought from the customer shall be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer shall be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

### 30.2 Secrecy Obligations and Sharing of Information:

30.2.1 Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

30.2.2 While considering the requests for data/ information from Government and other agencies, Bank 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 in the banking transactions.

The exceptions to the said rule shall be as under:

- a. Where disclosure is under compulsion of law.
- b. Where there is a duty to the public to disclose.
- c. The interest of Bank requires disclosure and
- d. Where the disclosure is made with the express or implied consent of the customer.

### 30.2.3 Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

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

### 30.3 Hiring of Employees and Employee Training

#### a. Screening Mechanism for Personnel Recruitment:

As part of our commitment to ensuring a robust KYC/ AML/ CFT framework, we have established an adequate screening mechanism, including a comprehensive Know Your

Employee/ Staff policy, to be followed during the personnel recruitment and hiring process. This mechanism aims to identify individuals with high integrity and ethical standards who can effectively contribute to our efforts in combating financial crimes.

b. Competency and Training of Staff:

We strive to maintain a workforce that possesses a deep understanding of the prevailing KYC/ AML/ CFT standards and regulations, both nationally and internationally. Our staff members involved in KYC/ AML/ CFT matters undergo a rigorous selection process to ensure they possess the necessary expertise, effective communication skills, and the ability to adapt to the evolving landscape of KYC/ AML/ CFT practices.

Furthermore, we foster an environment that encourages open communication and emphasizes the importance of high integrity among all our staff members.

c. Ongoing Employee Training Program:

To ensure that our staff members are equipped with the latest knowledge and skills required for effective KYC/ AML/ CFT implementation, we have established an ongoing employee training program. This program is designed to address the specific needs of different categories of staff members, including frontline staff, compliance staff, and those dealing with new customers.

The training program focuses on enhancing customer education capabilities for frontline staff and covers various aspects of KYC/ AML/ CFT policies and procedures. We also prioritize the development and continuous training of our compliance staff to stay updated with regulatory requirements and emerging trends.

d. Adequate Staffing of the Audit Function:

We recognize the importance of maintaining an independent and effective audit function within our organization. To achieve this, we ensure that our audit function is staffed with individuals who possess a thorough understanding of our KYC/ AML/ CFT policies, relevant regulations,

and related issues. These individuals are adequately trained to perform audits and assessments to ensure compliance and identify areas for improvement.

#### 30.4 Accounts under Foreign Contribution Regulation Act, 2010 (FCRA):

30.4.1 In terms of the Foreign Contribution Regulation Act, 2010, certain categories of individuals and organizations are required to obtain prior permission from the Central Government (Secretary, Ministry of Home Affairs, GOI, New Delhi) to receive “Foreign Contributions” or accept “Foreign Hospitality” and such receipts/acceptance require reporting to the Government.

30.4.2 Individuals/ Organizations who cannot receive foreign contributions: Foreign contributions cannot be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employee of any corporation, member of any legislature, political party or office bearer thereof.

30.4.3 Individuals/ Organizations who can receive foreign contributions: An association having a definite cultural, economic, educational, religious or social programme can receive foreign contribution after it obtains the prior permission of the Central Government or gets itself registered with the Central Government.

30.4.4 Banks can credit any foreign contribution to accounts of Association/ Organisation only if it produces documentary evidence for having obtained registration / prior permission from the Central Government. Hence, it is mandatory that Associations / Organisations have to be registered with the Central Government for receiving foreign contributions.

It is also mandatory that the foreign contributions are credited only to designated FCRA

Accounts with relevant FCRA registration number provided by Ministry of Home Affairs, Government of India. No other credits should be permitted in such FCRA designated accounts. Funds flow from the Donor Agencies placed under Prior Reference Category (PRC) by MHA to any person, NGO / Organization in India be brought to the notice of MHA and the funds are allowed to be credited into the account of the recipient only after clearance / prior permission from the Ministry of Home Affairs, Govt. of India.

30.4.5 Bank shall ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

30.5 Designated Director on the Board of the Bank:

- a. Designated Director:
  - i. Definition: A "Designated Director" refers to a person designated by our bank to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The Designated Director shall be nominated by the Board.
  - ii. Communication to FIU-IND: The name, designation, and address of the Designated Director shall be communicated to the Financial Intelligence Unit - India (FIU-IND).
  - iii. Communication to RBI: Additionally, the name, designation, address, and contact details of the Designated Director shall be communicated to the Reserve Bank of India (RBI).

**Principal Officer Exclusion:** It is important to note that the Principal Officer shall not be nominated as the Designated Director under any circumstances.

30.6 Principal Officer:

- a. Principal Officer:



- i. Responsibilities: The Principal Officer of our bank shall be responsible for ensuring compliance with KYC requirements, monitoring transactions, and facilitating the sharing and reporting of information as mandated by applicable laws and regulations.
- ii. Communication to FIU-IND: The name, designation, and address of the Principal Officer shall be communicated to the Financial Intelligence Unit - India (FIU-IND).
- iii. Communication to RBI: Additionally, the name, designation, address, and contact details of the Principal Officer shall be communicated to the Reserve Bank of India (RBI).

b. Responsibilities of the Principal Officer:

The Principal Officer shall assume the following responsibilities to ensure effective implementation of the bank's KYC policy:

- i. Compliance Oversight: Oversee the bank's compliance with KYC regulations and internal policies.
- ii. Transaction Monitoring: Monitor customer transactions for any suspicious activities and promptly report any findings in accordance with applicable laws and regulations. The Principal Officer under the Prevention of Money Laundering Act, 2002 shall serve as the competent authority for establishing the thresholds for the generation of Anti-Money Laundering (AML) alerts.
- iii. Information Sharing: Facilitate the sharing of information related to suspicious transactions with appropriate regulatory authorities and the FIU-IND as required.
- iv. Reporting Obligations: Ensure timely reporting of suspicious transactions and the fulfillment of reporting obligations in accordance with the provisions of the law and regulations.
- v. Training and Awareness: Conduct regular training programs for bank employees to enhance their understanding of KYC requirements and facilitate adherence to the bank's policies.
- vi. Regulatory Updates: Stay updated with the latest regulatory developments, amendments, and guidelines related to KYC and ensure their incorporation into the bank's policies and procedures.

- vii. Internal Controls: Establish and maintain robust internal controls and systems to detect and prevent money laundering, terrorist financing, and other illicit activities.

Reporting and Communication: The Principal Officer shall maintain effective communication channels with regulatory authorities, including the FIU-IND and the RBI. Any communication or reporting requirements shall be fulfilled promptly and accurately.

#### 30.7 Need for photographs and address confirmation:

30.7.1 Pass port size/ stamp size photograph of the depositors shall be obtained in case of all Current Accounts, SB accounts and Term Deposits.

30.7.2 In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public/ private limited companies, HUF, trusts, Limited Liability Partnerships etc., and those of minors, photographs of the authorised signatories should be obtained. Photographs of the student account holders should be attested by the school authorities on the reverse.

30.7.3 In case of change in the authorised signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organisations.

30.7.4 Photograph should be obtained in case of NRI accounts also.

30.7.5 Where the accounts are operated by letters of authority, photographs of the authority holders should be obtained, duly attested by the depositors.

#### 30.8 Sale of third party products:

30.8.1 When Bank sells third party products as agent, the responsibility for ensuring compliance with KYC/ AML/ CFT regulations lies with the third party. However, to mitigate reputational risk to Bank and to enable a holistic view of a customer's transactions, branches are advised as follows:

(a) Even while selling third party products as agents, branches should verify the identity and address of the walk-in customer.

(b) Branches should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in paragraph 6 above (Maintenance of KYC documents and preservation period).

(c) Bank's AML software will capture, generate and analyse alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers.

d) Sale of third party products by branches as agents to customers, including walk-in customers, for Rs.50,000 and above must be (a) by debit to customer's account or against cheques and (b) obtention & verification of the PAN given by the account based as well as walk-in customers. This instruction would 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 Rs. 50,000/- and above.

30.9 KYC check for new Technology products- Net Banking / Credit Cards / Debit Cards / Gift Cards / Forex cards.

30.9.1 Branches should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. We are also introducing a variety of Electronic Cards that are used by

customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Branches are required to ensure full compliance with all KYC / AML / CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards may be done through the services of agents. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

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

##### CDD Procedure and Sharing KYC Information with Central KYC Records Registry (CKYCR)

###### a. Authorization and Regulatory Framework:

- i. The Government of India has authorized the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) to act as the Central KYC Records Registry (CKYCR) as per Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- ii. In accordance with Rule 9(1A) of the Prevention of Money Laundering (Maintenance of Records) Rules, the Bank shall capture customer's KYC records and upload them onto the CKYCR within 10 days of establishing an account-based relationship with the customer.
- iii. Operational guidelines for uploading KYC data have been released by CERSAI.

###### b. KYC Information Sharing:

- i. The Bank shall capture the KYC information of customers to be shared with the CKYCR as per the guidelines mentioned in the Rules. This includes using the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), which may be revised by CERSAI from time to time.

- ii. The CKYCR's "live run" commenced on July 15, 2016, with a phased approach starting with new 'individual accounts.' Consequently, the Bank is required to upload KYC data for all new individual accounts opened on or after January 1, 2017, to the CKYCR. SCBs were initially given time until February 1, 2017, to upload data for accounts opened in January 2017.
- iii. The Bank shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with the CKYCR, as per the provisions of the Rules. The KYC records should be uploaded using the LE Template released by CERSAI.
- iv. Upon generation of a KYC Identifier by the CKYCR, the Bank shall ensure that the same is communicated to the respective individual/ LE.
- v. To ensure incremental uploading of all KYC records onto the CKYCR, the Bank shall upload/ update the KYC data of individual customers and LEs who opened accounts prior to the mentioned dates (in points ii and iii, respectively) during periodic updates as specified in Section 20 of the KYC Policy. The Bank may also upload/ update the KYC data earlier when updated KYC information is obtained/ received from the customer. Also, whenever 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 RE 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.
- vi. During periodic updation, the Bank shall ensure that customers are migrated to the current Customer Due Diligence (CDD) standard.
- vii. In cases where a customer submits a KYC Identifier to the Bank, with explicit consent to download records from the CKYCR for the purpose of establishing an account-based relationship, the Bank shall retrieve the KYC records online from the CKYCR using the provided KYC Identifier. In such instances, the customer shall not be required to submit the same KYC records or information, or any additional identification documents or details unless:
  - (i) There is a change in the customer's information as existing in the CKYCR records.

- (ii) Verification of the current address of the customer is necessary.
- (iii) The Bank considers it necessary to verify the identity or address of the customer, perform enhanced due diligence, or build an appropriate risk profile of the client.
- (iv) The validity period of documents downloaded from CKYCR has lapsed.

#### 30.11 Period for presenting payment instruments

30.11.1 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.

#### 30.12 Collection of Account Payee Cheques

30.12.1 Account payee cheques for any person other than the payee constituent shall not be collected. Banks shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

30.13 The Depositor Education and Awareness Fund Scheme, 2014 –Section 26A of Banking Regulation Act, 1949 - Due diligence of customers who claim the amount.

30.13.1 As per RBI Circulars DBOD No DEAF Cell BC 101/30.01.002/2013 – 14 dated 21.3.2014 and DBOD No DEAF Cell BC 114/30.01.002/2013 – 14 dated 27.5.2014, Reserve Bank of India has informed Banks that it has been decided to establish a “Depositor Education and Awareness Fund” (DEAF).

30.13.2 As per the direction contained therein, Banks will have to transfer to the DEAF account, the amount to the credit of any account in India with a banking company which has not been operated upon for a period of ten years or any deposit or any amount

remaining unclaimed for more than ten years. The depositor would, however, be entitled to claim from the bank his/her deposit or any other unclaimed amount or operate his/her account after the expiry of ten years, even after such amount has been transferred to the Fund.

30.13.3 As per RBI Circular No. RBI/2014-15/311 DBR.No.DEA Fund Cell.BC.49/

30.01.002/ 2014-15 Dated November 21, 2014, Bank needs to carry out proper due diligence as per the risk category of the customers before making payments to the customers who approach the Bank claiming the amount that is already transferred to the DEAF scheme. Due diligence would mean ensuring genuineness of the transaction, verification of the signature and identity, etc.

### 31. **Annexure 1**

List of Low/ Medium/ High risk Customers based on the recommendations of IBA Working Group.

The categorization of customers under risk perception is only illustrative and not exhaustive.

### 32. **Annexure 2**

#### 32.1 High / Medium Risk Products and Services

32.1.1 Branches / Offices are required to pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Presently a variety of Electronic Cards are used by customers for buying goods and services, drawing cash from ATMs, and for electronic transfer of

funds. Branches should ensure that appropriate KYC procedures are duly applied before issuing the Cards including Add-on / Supplementary Cards to the customers.

### 32.2 Indicative list of High / Medium Risk Products and Services

1. Electronic funds payment services such as electronic cash (e.g., stored value and pay roll cards), funds transfer (domestic and international) etc.
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6. Foreign correspondent accounts
7. Trade finance (such as letters of credit)
8. Special use or concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities
10. Non-deposit account services such as Non-deposit investment products and Insurance
11. Transactions undertaken for non-account holders (occasional Customers)
12. Provision of safe custody and safety deposit boxes
13. Currency exchange transactions
14. Project financing of sensitive industries in high-risk jurisdictions
15. Trade finance services and transactions involving high-risk jurisdictions
16. Services offering anonymity or involving third parties
17. Services involving banknote and precious metal trading and delivery
18. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.



### 33. **Annexure 3**

#### 33.1 High / Medium Geographic risk

33.1.1 Branches/offices are required to prepare a profile for all new customers based on risk categorization, taking into account the location of the customer and the customer's clients as well as factors such as the nature of business activity, mode of payments, turnover and customer's social and financial status including location of his business activity and to exercise due diligence based on the bank's risk perception.

33.1.2 The customer should be subjected to higher due diligence if following criteria falls under "high-risk" geographies

- Country of nationality (individuals)
- Country of residential address (individuals)
- Country of incorporation (legal entities)
- Country of residence of principal shareholders / beneficial owners (legal entities)
- Country of business registration such as branch/liaison/project office
- Country of source of funds
- Country of the business or correspondence address
- Country with whom customer deals (e.g. 50% of business – trade, etc.)

33.1.3 Apart from the risk categorization of the countries, branches/ offices should categorize the geographies/ locations within the country on both Money Laundering (ML) and Financing Terrorism (FT) risk.

#### 33.2 Indicative List of High / Medium Risk Geographies Countries/Jurisdictions

1. Countries subject to sanctions, embargos or similar measures in the United Nations Security Council Resolutions (“UNSCR”).
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks ([www.fatf-gafi.org](http://www.fatf-gafi.org))
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies ([www.fatf-gafi.org](http://www.fatf-gafi.org))
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
5. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
6. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
7. Countries identified by credible sources as having significant levels of criminal activity.
8. 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

1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations/cities and affected districts)
2. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
3. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

NOTE: Risk assessment should take into account following risk variables specific to a particular customer or transaction:

- The purpose of an account or relationship
- Level of assets to be deposited by a particular customer or the size of transaction undertaken.
- Level of regulation or other oversight or governance regime to which a customer is subjected to.
- The regularity or duration of the relationship.
- Familiarity with a country, including knowledge of local laws, regulations and rules as well as structure and extent of regulatory oversight.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or increase the complexity or otherwise result in lack of transparency.

#### 34. **Annexure 4**

34.1 Monitoring of Customer Risk Categorisation (CRC): As per internal and regulatory guidelines.

#### 35. **Annexure 5**

35.1 List of documents to be collected for Account opening – Details

35.1.1 Opening of Accounts of Individuals

Where the client is an individual, while establishing an account – based relationship, or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney related to any legal entity, he shall submit:

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

or

(aa) the proof of possession of Aadhaar number where offline verification cannot be carried out or any other Officially valid document (OVD) or the equivalent e-document thereof containing the details of his identity and address: and

(b) the Permanent Account Number (shall be verified from the verification facility of the issuing authority) or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, and

such other documents including in respect of the nature of business and financial status of the client, or equivalent e-documents thereof as may be required by the reporting entity/ Bank.

As per the Fifth amendments to PML Rules, 2005 dated 13.11.2019, the 'Officially Valid Documents' (OVD) means

- 1) The Passport
- 2) The Driving License
- 3) Proof of possession of Aadhaar number
- 4) The Voters' Identity card issued by Election Commission of India
- 5) Job card issued by NREGA duly signed by an officer of the state government
- 6) The letter issued by National Population register containing details of name, and address

Any other document as notified by Central Government in consultation with the regulator.

Provided that,

- a) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such a form as are issued by the Unique Identification Authority of India.
- b) In case of officially valid document furnished by the client does not contain updated address, the following documents or equivalent e-documents thereof shall be deemed to be officially valid documents for the limited purpose of proof of address: -

- 1) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
  - 2) property or Municipal tax receipt;
  - 3) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
  - 4) 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;
- c) The customer shall submit updated Officially Valid Document with current address within a period of three months of submitting the above documents.
- 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

#### Features to be verified – Proof of Identity and Proof of Address

Bank at the time of commencement of an account-based relationship-

- a) Identify its clients, verify their identity, obtain information on the purpose and intended nature of the business relationship; and
- b) determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner:

Document to be obtained and verified

- i. One Recent Photograph
- ii. Where the customer is a Resident individual, he /she shall submit;
  - (a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under the 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

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

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any other Officially valid document (OVD) or the equivalent e-document thereof containing the details of his identity and address: and

(b) the Permanent Account Number (shall be verified from the verification facility of the issuing authority) or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules.

Every reporting entity shall, where its client submits his Aadhaar number, ensure such clients to redact or blackout his Aadhaar number through appropriate means where authentication of Aadhaar number is not required under sub rule 15 ie, he is not desirous of receiving any benefits or subsidies under section 7 of Aadhaar act.

The e-KYC service of UIDAI shall be accepted as valid process of KYC Verification under PML Rules as

i) the information containing demographic and photographs made available from UIDAI and

ii) transfer of KYC data, electronically to the Bank from UIDAI

are accepted as valid process of KYC verification, subject to the condition that the necessary authorisation from the Individual customer authorising UIDAI by way of explicit consent is obtained to release his/her identity and address through e-KYC or Yes /No Authentication to the Bank.

Where a customer, for the above purposes submits a KYC Identifier to the Bank, then Branch shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require the 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 Central KYC Records Registry;
- ii) the updated address of the customer is required to be verified;
- iii) the Bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

### 35.2 Sole Proprietorship Relationships

Business Firm/s started by an Individual or a legal person i.e. Limited Company or as a unit of a HUF is/are classified as Sole Proprietorship Firms.

Reserve Bank of India has laid down criteria for Customer Identification Procedure for Account Opening by Proprietary Concerns.

Customer Identification Procedure as applicable to the Individual proprietor. i.e., Branch shall call for and verify certified copies of

1. One copy of an officially valid document containing details of identity and address, one recent photograph and PAN of the Individual (Proprietor) or the equivalent e-document thereof and
2. 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:
  - a. Registration certificate
  - b. Certificate/license issued by the municipal authorities under Shop and Establishment Act.

- c. Sales and income tax returns.
- d. CST/ VAT/ GST Certificate (provisional/final)
- e. Certificate/registration document issued by Sales tax/Service tax/professional tax authorities
- f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ license/ certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- g. 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.
- h. Utility bills such as electricity, water, and landline telephone bills.

These documents should be in the name of the proprietary concern.

In case, where the Bank is satisfied that it is not possible to furnish two such documents, Bank may at our discretion, accept any one of those documents as proof of business/activity. In such a case it is imperative that Contact Point Verification is made and shall confirm and satisfy under record to establish that the activity of the proprietary concern is carried on at the address of the proprietary concern.

### 35.3 Accounts of Partnership Firms

For opening of Partnership firm, one certified copy or the equivalent e-documents of the following documents be obtained.

Features to be verified – Legal Name, Address of Firm, Activity of the Firm, Names, Address of partners and Beneficial owner/s and telephone Number of the Firm and partners.

Please note that accounts of partnership Firm where HUF happens to be one of the partners, cannot be opened. (Ref. Cir. No. ADV / 71 / 2004-05 Dt. 28 January, 2005).



Documents to be obtained and verified

Recent Passport size colour photograph of the Partners/Authorised signatories / Beneficial Owners (Partners who are having 15% or more share in the Partnership firm)

Where the client is a partnership firm, it shall submit the certified copies of the following documents

- i) registration certificate (if registered)
- ii) partnership deed; and
- iii) PAN in the name of the Partnership Firm, shall be verified from the verification facility of the issuing authority.
- iv) Where Registration of the Partnership Deed is not done, in lieu of Registration Certificate, Branch to obtain on best effort basis
  - 1. CST/ VAT/ GST Certificate (provisional/final)
  - 2. Import-Export Code issued by DGFT
- v) Documents as specified in the Section 4.2.(b) above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

#### 35.4 Private/ Public Limited and ONE PERSON COMPANY (OPC)

Features to verified – Name of the Company, principal place of business, Address of the Company, Activity of the company, Names & Address of Directors, Directors Identification Number (DIN), Company Identification Number (CIN), whether the Company is in Active Status as per MCA site, Power of Attorney Holder/s / Authorised Signatories and Beneficial owner/s, Telephone Number / Fax number.

Documents to be obtained and verified

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

- a. A resolution from the Board of Directors and Power of Attorney granted to its managers / officers / employees to transact on its behalf, duly certified as True copy by one of the present Directors (other than the Director/s who is an authorized Signatory) or Company Secretary.
- b. Permanent Account Number (PAN) (shall be verified from the verification facility of the issuing authority) is mandatory or the equivalent e-document thereof
- c. Latest Copy of Certificate of Incorporation and Certificate of Commencement, Memorandum of Association (MOA), Articles of Association (AOA) verified with original.
- d. For companies Regd. Under Sec. 25 /Sec. 8 of Companies Act 2013, Copy of the certificate issued by the Ministry of Company Affairs exempting the company from using the words like “Private”, “PVT”, “(P)”, “Limited” to their NAME.
- e. Copy of documents as specified in the Section 4.2. (b). above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- f. Photo, one copy of an officially valid document containing details of identity and address, PAN or Form 60 as defined in Income Tax Rules 1962 of the Beneficial Owner/s (i.e. Share Holders who are having 25% or More shares in the Company)
- g. Online verification of MCA site to confirm that the name of Directors as per site is the same as shown in the a/c opening form and the company is in 'Active Status' as per site. Necessary Due Diligence be done to ensure that the company is not having the features of a Shell Company as defined elsewhere in the Policy
- h. Communication Address Proof in the name of company to be collected, if address is different / not mentioned in Certificate of Incorporation.

- i. Registered Address Proof in the name of company to be collected.

### 35.5 Hindu Undivided Family

Features to be verified– Legal Name, Name and address of Karta/ Co-parceners.

Documents to be obtained and verified

Certified copies of

- a. Existence Proof of the entity – PAN is a MUST for this and the account title will be as it appears on the PAN.
- b. Latest photo, OVD and PAN or Form No.60 of the Karta
- c. One copy of an officially valid document containing details of identity and address, and one recent photograph and PAN /Form 60 of the Co-parceners who have attained the age of majority.
- d. For Current account opening
  - i) the business communication address proof.
  - ii) CST/ VAT/ GST Certificate (provisional/final)
- e. Updated Residential Address Proof of the Karta and Co-parceners, who have attained majority.

### 35.6 Trusts / Foundations

Features to be verified- Legal Name, Names of trustees, settlers, beneficiaries and signatories, Beneficial Owners

Documents to be obtained and verified.

Documents as per Rule 9(8) of Prevention of Money Laundering June 2017 are to be obtained

i.e.

Certified copy of following documents or the equivalent e-documents of thereof shall be obtained:

- a. Registration Certificate
- b. Trust Deed and PAN (shall be verified from the verification facility of the issuing authority) or Form 60 of the trust
- c. One copy of an officially valid document containing details of identity and address, one recent photograph and PAN (shall be verified from the verification facility of the issuing authority)/ Form No. 60 in respect of the person holding a Power of Attorney to transact on its behalf.
- d. Where the Trust / Foundation is not having the Registration Certificate, Permanent Account Number in the name of the Trust /Foundation be obtained for Existence Proof.
- e. Along with the Trust Deed, addendum/ supplement deed, if any should also be collected.
- f. List of the Present Trustees, duly signed by one of the trustees or the Settler.
- g. Resolution passed by the trustees to open the account with the Bank.
- h. Resolution passed by the Trustees authorizing / mentioning the mode of operation of the account.
- i. Legal opinion from banks panel lawyer or from the Legal officer of the bank, clearly mentioning
  - a) that there are no onerous clauses in the Trust Deed
  - b) whether Bank can open the account
  - c) the mode of operation of the account as per the Trust Deed.
- j. Sanction/approval from the respective Regional Head for opening the account.
- k. PAN or Form 60 of the Trust duly filled up and signed by a present Trustee
- j. Photo, copy of documents as specified, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- l. Communication addresses proof of the Trust.

- m. Indemnity letter in prescribed stamp paper (Format A9), signed by all the Trustees in their fiduciary capacity i.e., with rubber stamp/seal.

### 35.7 Limited Liability Partnership registered under LLP Act 2008

Features to be verified – Legal Name, Designated Partners, activity

Documents to be obtained and verified - Certified copies of

- a. LLP agreement signed by all designated Partners on all pages under authority stamp.
- b. Certificate of registration/Incorporation obtained from ROC in the name of LLP for establishing the identity of LLP (Either newly incorporated LLP or conversion from existing Partnership Firm/ Private Ltd or Unlisted Public Ltd).
- c. Resolution to open and operate the account specifying the Name of the Bank, Nature of account to be opened and the person authorised to open and operate the Bank account, duly certified by the Chairman of the meeting.
- d. One copy of an officially valid document containing details of identity and address and one recent photograph, PAN / Form 60 of the Authorised Signatories for account operations. If the Individual holding an attorney to transact on the Entity's behalf is not eligible to be enrolled for Aadhaar number, certified copy of an officially valid document be obtained
- e. Communication Address Proof in the name of LLP, if such address different / not mentioned in documents collected under point (b).
- f. Registered Address Proof in the name of LLP to be collected, if address is different from document collected.
- g. Permanent Account Number (PAN)
- h. Latest List of all Designated Partners with their addresses and their DPIN (Designated Partners Identification Number) signed and dated by the CA/CS/Designated partner/s. Proof of

appointment of designated partners which are mentioned in latest list of designated partners, but appointed after incorporation of LLP.

i. CST/ VAT/ GST Certificate (provisional/ final)

35.8 Unincorporated Bodies, Association of Persons or Body of Individuals like Clubs, Associations, etc.

#### 35.8.1 Association of Persons (AOP)

Under the Income Tax Act., an Association of Persons (AOP) is an entity or unit of assessment. It means two or more persons who join for a common purpose with a view to earn an income. The term PERSON includes any company or association or body of individuals, whether incorporated or not. The association need not be on the basis of contract. Therefore, if two or more persons join hands to carry on a business, but do not constitute a partnership they may be assessed as an AOP. But an AOP does not mean any and every combination of persons. It is only when they associate themselves in an income-producing activity that they become an association of persons.

#### 35.8.2 Body of Individuals (BOI)

Body of Individuals (BOI) means a conglomeration of individuals who carry on some activity with the objective of earning some income. It would consist only of individuals. Entities like companies or Firms cannot be members of body of individuals. Income Tax shall not be payable by an Assessee in respect of the receipt of share of income by him from BOI and on which the tax has already been paid by such BOI.

Difference between AOP & BOI

- a) An AOP may consist of non-individuals. If two or more persons (like firm, company, HUF, individual, etc.) join together, it is called an AOP.
- b) An AOP implies a voluntary getting together for a common purpose or combined will to engage in an income producing activity,
- c) BOI has to consist of individuals only, i.e., natural persons. But if only individuals join together, then it is a BOI.
- d) BOI may or may not have a common purpose or will.

The documents as per Rule 9 (9) of Prevention of Money Laundering (maintenance of records) to be obtained are;

Certified copy of following documents or the equivalent e-documents of thereof shall be obtained:

- 1) Resolution of Managing Body of such association or body of individuals
- 2) Power of Attorney granted to him/her to transact on its behalf
- 3) Copy of documents as specified in the Section 4.2. (b). above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- 4) PAN (shall be verified from the verification facility of the issuing authority) or Form 60 of the unincorporated association or body of individuals
- 5) Such information as may be required to collectively establish the legal existence of such association / body of individuals/ Association of Persons

Additionally, the following documents are also be collected.

- 6) Copy of the Rules or Bye Laws;
- 7) The list of the present office Bearers along with a copy of minutes of the General Body meeting electing the present Office bearer
- 8) Communication Address Proof in the name of the unincorporated body.

### 35.9 Juridical Persons – Documents to be obtained as part of Customer Due Diligence (CDD)

A juridical person is a legal entity created by the law which is not a natural person, such as a corporation created under State statutes. It is a legal entity having a distinct identity and legal rights and obligations under the law.

For opening accounts of Juridical Persons such as Government or its Departments, Societies, Universities and Local Bodies like village panchayat, etc., certified copies of the following documents or the equivalent e-documents of thereof shall be obtained.

- (a) Document showing name of the person authorised to act on behalf of the entity;
- (b) Any Officially valid document containing details of identity and address, PAN or Form 60 in respect of the person holding an attorney to transact on its behalf and
- (c) Such documents as may be required to establish the legal existence of such an entity/ juridical person.

### 35.10 Self Help Groups (SHG) / Joint Liability Group

To promote thrift /savings habits and to encourage people to engage in productive activities to earn a livelihood, mainly among the low income group in rural/ semi urban areas, the concept of Self Help Group (SHG) are promoted among people from local area / same locality. They are encouraged to form peer groups with a maximum of 20 persons.

#### Joint Liability Group (JLG)

JLG is a group of 4 to 10 Individuals of same village or locality of homogenous nature and of the same socio-economic background, who mutually come together to form a group for the purpose of availing loan from Bank.



Some of the SHGs/ JLGs are promoted by NGOs. Such NGOs may have got necessary certification from NABARD as a Self-Help Promoting Institutions (SHPI), The sponsoring letter from such NGOs, can be construed as an Existence proof for SHGs/ JLGs.

Difference between SHGs and JLGs

Size – Up to 20 members for SHGs

4 to 10 members for JLGs

Nature of Loan - Single loan to the SHG as a whole, which decides how it should be allocated.

Whereas for JLGs, the Loan is recorded in the names of Individual borrowers.

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening savings bank accounts and credit linking of their accounts, RBI has simplified certain norms for SHGs as under:

KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice.

As regards KYC verification at the time of credit linking of SHGs, it is clarified that since KYC would have already been verified while opening the savings bank account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary. (Ref: RBI/2012-13/459 DBOD.AML.BC. No.87/14.01.001/2012-13 March 28, 2013).

Documents to be obtained and verified

Certified copy of

- a. Group Formation minutes indicating the election of Office bearers, Name of SHG/ JLG
- b. Bye Law of the SHG/JLG, duly certified by the sponsoring Agency like NSS, SNDP Yogam, Amritha, etc. along with the sponsorship letter
- c. The copy of the minutes, showing the decision to open relationship with the Bank.

d. Copy of any officially valid document containing details of identity and address, one recent photograph and Form 60/PAN of the Office Bearers

e. PAN or Form 60 in the name of the SHG/JLG duly filled up and signed by any two the Office Bearers with seal.

#### 35.11 Minors who have attained the Age of TEN or above

Features to be verified- Legal Name and Address.

Documents to be verified and obtained.

Certified copy of

- a. Any Officially valid document containing details of identity and address, one recent photograph and PAN of the Minor, if available (for Minors of the Age of TEN and above only)
- b. Proof of Date of Birth of the Minor, if not available in Aadhaar.
- c. PAN or Form 60 of the Guardian, if the Minor is not having PAN
- d. Any Officially valid document containing details of identity and address, one recent photograph and PAN/ Form 60 of the Guardian (for accounts operated by Guardian)
- e. Where the address on the Aadhaar is not the Current Address, the OVD can be accepted for the limited purpose of current Address proof.

#### 35.12 Societies

A Co-operative Society functions as per the provisions of below mentioned articles:

- 1 Co-operative Societies Act under which the same is registered.
- 2 Co-operative Societies rules made there under
- 3 Bye-laws approved by the registrar at the time of registration and amendments made from time to time and approved by the registrar.
- 4 Notification and Orders

When the area of operation is restricted to one State, the State Co-operative Act & Rules, under which the society is registered, will be applicable. In a particular State, if Co-operative Act and Rules is not enacted, the Central Act which is known as The Co-operative Act, 1912 and its rules will be applicable. When the area of operation of Society is spread in two or more States, the Multi-State Co-operative Societies Act, 2002 and its rules shall be applicable.

As regards investment of funds/ deposits, in certain States, the respective Co-operative societies Act passed by the State Legislature Assembly envisages to obtain approval of District Registrar, appointed under the Act.

Features to be verified - Legal name of the Society, its Office Bearers and address

Documents to be obtained and verified.

Certified copy of

- a. Latest Bye Laws / MOA, etc.
- b. Certificate of registration
- c. List of the present office bearers along with the minutes of the last General body meeting electing them
- d. Any Officially valid document containing details of identity and address, one recent photograph and PAN/ Form 60 of all authorised signatories.
- e. Copy of PAN of the Society
- f. Certified copy of Board / Managing Committee / Governing Body Resolution
- g. Address Proof of the entity.
- h. Necessary approval from the District Registrar, wherever applicable

(Applicable in States like Kerala, Tamil Nadu, Karnataka, Maharashtra. etc.).

### 35.13 Accounts of Executor and Administrators

Documents to be verified and obtained

Certified copy of

- a. the Will of the Testator i.e. the person who expired leaving a Will.
- b. If the Will is registered, the proof for registration
- c. If the Will is not Registered, Probate of the Will is to be obtained. Alternatively, a declaration from all the legatees [beneficiaries] of the Will declaring that the Will dated ..... is the last one and is in existence and they have no objection in opening a CD /SB account as proposed in the said Will.
- d. Any Officially valid document containing details of identity and address, one recent photograph and PAN /Form 60 of the Executors/ Administrator
- e. Address Proof (under officially valid document) of the Executors/ Administrators, if the address is different from the Aadhaar

35.14 Institutions constituted under separate Statutes passed in Assembly/Parliament – e.g. Welfare Boards, LIC, etc./Govt. Bodies /Departments / Govt. owned PSUs/Companies

Documents to be obtained

Certified copy of

- a. Permanent Account Number (PAN), wherever applicable.
- b. The Certified copy signed by the Chairperson / Chairman / Co-Chairman / Vice-Chairman / Member Secretary / Managing Director / authorized signatory (For Government Body / Board / Corporation / Funds of the State Govt.), as per the powers mentioned in the Act / bye laws of such entities.
- c. Any Officially valid document containing details of identity and address, one recent photograph and PAN or Form 60 of Authorised Signatory(ies)
- d. Address proof of Entity.

e. Statutory boards of the Government are governed by a Body / Cabinet Committee and an executive committee such as, Infrastructure Development Board, Development Funds, and Welfare Funds of Govt. The Member Secretary as Convener of the Governing Council Cabinet Committee and Chairman of Executive Committee acts as the focal point for all decisions (similar to the role played by a Company Secretary in case of Companies).

Owing to the role played by him, the resolution can be signed by Member Secretary for opening accounts after providing the linking document that authorizes him for opening accounts.

f. In case of Ex-Officio account or by designation account – such as Director (of a Govt Dept) / Civil Surgeon/ Senior Medical Officer, Drawing and Disbursing officer, Health Accounts, Municipality accounts, Government Dept / entities / boards, where the signatories are decided by the designation they hold – Board Resolution can be on letter head of the signatory, where in, he authorizes himself for the opening of the account, based on a Government Order / Gazette / Treasury rules / Bye laws / rules and regulations / notifications or an act, issued by the concerned State or Central Government, with a copy of such delegation. The designation should be confirmed by way of a Govt. issued written order or ID card mentioning same designation. In case the ID card shows a different designation, then relevant transfer order (self-attested copy) can be obtained as proof of such change in designation.

g. The resolution should contain information such as powers to open, operate, further delegation, if any, mode of operation with designated powers, list of authorized signatories with their designations.

h. In case of Government Companies / PSUs, wherever possible, Certified copy of Board Resolution (BR) to open accounts signed by Company Secretary or MD to be accepted. Signatures of Managing Director / Company Secretary/ Other Authorized Signatory to be

accepted along with principal document or extract of principal document that authorizes such persons to open accounts.

i. Entities having one-time Resolution regarding powers of the 'Authorized Officials' (like CMD, MD, etc.) to open accounts and do not mention any specific delegation of financial powers / Mode of Operation (MoP) for accounts. In such cases, MOP as such 'Authorized Officials' of the entity will be acceptable and request letter issued by them to the Bank naming officials for operation of the account should be considered as sufficient delegation of financial powers.

j. In Govt. entities it is a common practice to mention the MOP as "the account shall be operated by the following officials: A, B and C, besides the Chairperson..." where in practice the Chairperson actually isn't ever required to operate the account. BR issued by such entities without signatures of such officials in signature column on AOF to be accepted. Subsequently a letter for inclusion Chairperson Signature may be obtained duly signed by the authorized person.

k. Relevant extracts of act governing opening and operation of accounts duly attested by authorized signatories or a declaration stating applicability of such extracts, duly attested by authorized signatories to be accepted. Copy of extracts to be attached

l. In case of Ex Officio accounts, the clause of rules and regulations / Bye laws to be relaxed as they are the drawing and disbursing officer of their respective departments and as such have powers to open and operate the account of the Department / District / Zila Parishad office they officiate over.

m. Copies to be Self Attested as "True & Updated" by an authorized signatory

n. List of all office bearers / Trustees, to be obtained on the letterhead with Rubber Stamp of the Government Body, with their addresses, signed and dated by Managing Trustee / Chairperson / Secretary/ authorized signatories.

o. In case of Government Entities, any official memo/ letter/ resolution/ order/ Gazette copy signed by a Gazetted Officer directing opening of account(s) will serve as an identity proof for that account. If the same contains the address, then it will serve as an address proof also. However, the name and style of the account and address on the AOF should match with that on the Government document.

p. Any Officially valid document containing details of identity and address, one recent photograph and PAN or Form 60 of the authorized signatories,  
In addition to above, public domain information such as website printout with signature of authorised signatories can be accepted as address proof.

#### 35.15 Unincorporated Joint Venture between Two entities / Companies:

Public and Private Companies are awarded contracts and projects. These contracts and projects may be from Central / State / Quasi Government or any Indian PSU or Entities controlled by Government. In order to carry out such projects these companies partner with other Public or Private companies through Unincorporated Joint Venture. One of the Partner members of such joint venture should have an account with the Bank and who is desirous of opening an account in the name of Joint Venture.

Features to be verified- Legal name, activity, country of Origin, and address

Certified Documents to be obtained and verified are as below:

Individual Board Resolution from each Joint venture partner

- a. Duly executed / Notarised copy of Joint venture Agreement
- b. Joint venture Board resolution on stating mandate and mode of operation
- c. Joint venture PAN Card copy and JV address proof. Account will be opened in the name mentioned on PAN card with “Joint Venture” or “JV” as suffix.
- d. Joint venture address proof, the same can be in the name of lead partner.

e. Duly attested Memorandum of Association / Articles of association and Certificate of Incorporation for all Joint Venture partners.

f. Any Officially valid document containing details of identity and address, one recent photograph and PAN /Form 60 of authorised signatories to the account. If the Individual holding an attorney to transact on the Entity's behalf is not eligible to be enrolled for Aadhaar number, certified copy of an officially valid document be obtained.

g. Contract Award Letter, wherever applicable

In case any of the joint venture partner is a Foreign Company, following documents in addition to the above, it would also be required to obtain the following documents with an approval from Regional Head or above.

a. Documents pertaining to Incorporation of the entity duly notarized by embassy of the said foreign company in India only if the documents are in foreign language. Else copies notarized by Indian notary can be accepted.

b. Documents pertaining to delegation of Authority to authorized signatory

c. KYC of authorized signatory (Passport being mandatory) if foreign company is a signatory to Joint Venture account

d. SWIFT message from the Banker of the foreign company confirming Name, Address, Telephone and Fax number of foreign company.

e. Beneficial Owners of the foreign Company and their appropriate KYC/AML documents

#### 35.16 Scheduled Commercial / RRBs / Co-operative Banks

Certified copies of

(a) Permanent Account Number (PAN) is mandatory.

(b) Board Resolution (BR)



- (c) Any Officially valid document containing details of identity and address, one recent photograph and PAN / Form 60 of the Authorised Signatories.
- (d) Communication Address Proof in the name of company
- (e) For RRBs or co-operative Banks, the BR would be signed by person authorized in BR itself or as per internal policies / guidelines / Bye laws of the Bank. In absence of any specific guideline, BR to be signed by Chairperson / CEO / MD / an officer of the rank of GM or above.
- (f) Letter identifying the officials to operate the account duly signed by Company Secretary/ Authorized Signatory.
- (g) RBI license for UCBs. In case of State Apex or DCCBs, if RBI license is not available, a letter from NABARD addressing the entity as ‘Bank’ to be obtained as proof of acceptance of said entity as Bank.
- (h) Copy of rules and bye laws of the Bank signed by any director / secretary / chairman / General Manager / Administrator appointed by Registrar. There are Primary Co-op Societies using “Bank” added to their name and in such cases, they have to be treated as Co-op Societies only. In the case of RRBs, if bye-laws is not available, certified copy of Gazette notification can be taken.
- (i) For a Regional Rural Bank, a photocopy of the gazette notification attested by Director / Secretary / Chairperson / authorized signatory. In case the photocopy of the original gazette notification is not available due to passage of time, a letter from sponsor Bank confirming that the entity is Regional Rural Bank sponsored by it.
- (j) Board Resolution duly signed by person whose reference has been made in resolution itself for signing and forwarding copy of the resolution to the Bank. In absence of such reference, person should sign it / official empowered under bye-laws.
- (k) Where the two or more Regional Rural Banks are merged, the photocopy of the order of merger duly certified by Chairman or two directors or secretary of the merged entity need

to be submitted. The said document would also be sufficient proof for changing the name. Also be applicable in case of merger of two urban cooperative Banks upon receipt of photocopy of merger letter issued by RBI / Ministry of Finance / Central Registrar / Registrar for Department of Cooperation of State.

(l) Where the board of the Cooperative Bank is suspended / superseded by an order of the Registrar of Cooperative Societies or Court, the designated official with delegated powers can open / operate the account as per the directive of the Registrar of Cooperative Societies or Court. Latest List of all directors with their addresses signed by director/ secretary / chairperson / authorized signatory. Office Order /Power of Attorney (approved by the appropriate authority in the Bank) in the names of the individuals authorized to open and operate Bank accounts.

(m) Necessary approval from the District Registrar of Co-op Society to open Current Account with us (wherever applicable).

### 35.17 Muslim Wakfs

Wakf is a granting or dedication of any property in trust (movable or immovable) by a person professing Islam, for any purpose recognized by the Muslim Law as religious, charitable or pious.

A Wakf may be declared orally, by words of mouth or in writing. However, a written Wakf is always advisable. Besides, where the dedication relates to an immovable property, the Wakf deed must be in writing and registered as per requirements of the Transfer of Property Act and Indian Registration Act. Every Wakf is required to be registered with the Wakf Board.

Mutawalli means any person appointed, under any deed or instrument by which a wakf has been created or by a competent authority to be a mutawalli of a Wakf by virtue of any customs or who is a naib-mutawalli, khadim, mujawar, sajjadanashin, amin or other person appointed by a mutawalli.

For any subsequent changes, Branches may rely upon stipulations laid down in Bank's Circulars issued from time to time.

### 35.18 Basic Savings Bank Deposit Account

Eligibility:

1. Individuals only, either singly or jointly
2. Minors jointly with the guardian following the usual precautions
3. The account cannot be opened by HUFs, Association, and Trust, etc.
4. The holders of "Basic Savings Account" are not eligible for opening any other savings bank deposit account in the Bank and the existing account, if any, will be required to close within 30 days from the date of opening a Dhanam Basic Savings Bank Deposit Account.

Features to be verified - Name and address

Document to be obtained and verified –

a) One recent photograph and

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

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962;

### 35.19 Small Accounts

Documents to be obtained

a self-attested photograph and

affixation of signature or thumb print,

as the case may be, on the form for opening the account

Provided that-

- (i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;
- (ii) If 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.

#### 35.20 Walk-in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees twenty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified.

However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-, the Bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

NOTE: In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 Banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

#### 35.21 Client accounts opened by professional intermediaries

When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks

may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also at times maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the Branch, the Bank should still look through to the beneficial owners. Where the Bank rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the Bank.

Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc., who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. We should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits Branches' ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s should not be allowed to open an account on behalf of a client.

Where the banks rely on the 'Customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

### 35.22 Accounts of Politically Exposed Persons (PEPs)

The Bank may establish a relationship with Politically Exposed Persons (PEPs), whether as customers or beneficial owners, only after satisfying the following criteria in addition to the standard customer due diligence:

- a. The Bank must have appropriate risk management systems in place to identify whether the individual or beneficial owner is a PEP.
- b. The Bank must undertake reasonable measures to ascertain the source of funds/ wealth of the PEP.
- c. Approval from the Regional Head is required before opening an account for a PEP.
- d. All accounts held by PEPs are subject to enhanced monitoring on an ongoing basis.

If an existing customer or beneficial owner subsequently becomes a PEP, approval from the Regional Head is required to maintain the business relationship.

These instructions are also 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.

### 35.23 Foreign Students Studying in India

The following procedure has been issued by RBI for opening accounts of foreign students who are not able to provide an immediate address proof while approaching a bank for opening bank account.

- a) Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.
- b) provided that a declaration about the local address shall be obtained within 30 days of opening the account and the local address is verified, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution or alternative means of verification of local address may be adopted by banks like a visit to the place of residence under record (i.e., keeping a Site Verification Report or by sending a Letter under Speed Post with Ack. Due. , etc.)
- c) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs.50,000/-, pending verification of address.
- d) On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in RBI's Master Circular on Non-Resident Ordinary Rupee (NRO) Account and the provisions of FEMA 1999.
- e) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

## **36. Annexure 6**

### **36.1 Depository Accounts**

#### **36.1.1 For individuals (Non-Body Corporate)**

In-person verification of applicant(s) at the time of opening Depository account.

At the time of opening depository accounts, the staff of the Participant should establish the identity of the applicant(s) (including guardian in case of minor account) by verifying the photograph(s) affixed in the account opening form as well as proof of identity document(s), with the person concerned. Further, in case of joint accounts, 'in-person' verification needs to be carried out for all the holders of the account.

For Non-Resident Indian/ Foreign National accounts, if it is infeasible to carry out 'in-person' verification of the NRI/ FN Client by the staff and/or verify the original KYC documents (POI and Proof of Address i.e. foreign address, where the NRI/ FN is residing) along with PAN card, in such a situation,

- (a) the account opening form and photocopies of the KYC documents and PAN card should be duly signed by the account holder; and
- (b) photocopies of the KYC documents and PAN card is attested by any of the entities viz; Notary Public, Court, Magistrate, Judge, Local Banker, Indian Embassy / Consulate General of the country where NRI/FN is residing [outside India]; and
- (c) the attestation is to the effect that it has been verified with the originals.

Participants should open the depository accounts or accept the PAN card only after it is satisfied with the authenticity of the documents (POI, Proof of Address and PAN card).

Participants should obtain a photocopy of the PAN card of the person(s) seeking to open the account and verify the same with the original PAN card. Further, it should be compared with the name appearing on the website of the Income Tax Department (ITD). In case of joint accounts, verification of PAN has to be done for each of the joint holder.

Documents that can be collected as valid Proof of Identity

- I. Passport
- II. Proof of possession of Aadhaar number
- III. Voter ID Card



IV. Driving license

V. PAN card with photograph (Mandatory)

With a view to bring about operational flexibility and in order to ease the PAN verification process, the intermediaries may verify the PAN of their clients online at the Income Tax website without insisting on the original PAN card, provided that the client has presented a document for Proof of Identity other than the PAN card

VI. Identity card/document with applicant's Photo, issued by a) Central/State Government and its Departments, b) Statutory/Regulatory Authorities, c) Public Sector Undertakings, d) Scheduled Commercial Banks, e) Public Financial Institutions, f) Colleges affiliated to Universities (this can be treated as valid only till the time the applicant is a student), g) Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members and h) Credit cards/Debit cards issued by Banks.

VII. Unique Identification Number (UID) (AADHAAR)

As per the SEBI master Circular UID is not mandatory. Ref: Circular No. SEBI/HO/MRD/DP/CIR/P/2016/134 dated December 15, 2016.

VIII. e-KYC service launched by UIDAI shall also be accepted as a valid process for KYC verification. The information containing the relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as a valid proof of Identity.

With a view to bring about operational flexibility and in order to ease the PAN verification process, the intermediaries may verify the PAN of their clients online at the Income Tax website without insisting on the original PAN card, provided that the client has presented a document for Proof of Identity other than the PAN card.

#### 36.1.2 Documents that can be collected as valid Proof of Address

(Documents having an expiry date should be valid on the date of submission.)

- I. Ration card
- II. Passport
- III. Voter ID Card
- IV. Driving license
- V. Bank passbook / Bank Statement (Not more than two months old)
- VI. Verified copies of a) Electricity bills (not more than two months old), b) Residence Telephone bills (not more than two months old)
- VII. Self-declaration by High Court & Supreme Court judges, giving the new address in respect of their own accounts.
- VIII. Identity card/document with address, issued by
  - a) Central/State Government and its Departments,
  - b) Statutory/Regulatory Authorities,
  - c) Public Sector Undertakings,
  - d) Scheduled Commercial Banks, e) Public Financial Institutions,
  - e) Colleges affiliated to universities (this can be treated as valid only till the time the applicant is a student) and g) Professional Bodies such as ICAI, ICWAI, Bar Council etc., to their members.
- IX. Proof of address issued by any of the following: Bank Managers of Scheduled Commercial Banks/Scheduled Co-Operative Bank/Multinational Foreign Banks/Gazetted Officer/Notary public/ elected representatives to the Legislative Assembly/Parliament/Documents issued by any Govt. or Statutory Authority.
- X. The proof of address in the name of the spouse may be accepted.
- XI. Aadhaar Letter issued by UIDAI shall be admissible as Proof of Address in addition to Proof

XII. e-KYC service launched by UIDAI shall also be accepted as a valid process for KYC verification. The information containing the relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as a valid proof of address

36.1.3 In case of joint holdings, Proof of Identity and Proof of address documents must be collected in respect of all the account holders

DP shall ensure that all documents pertaining to proof of identity and proof of address are collected from all the account holders. Submission of the aforesaid documents is the minimum requirement for opening a BO Account. DPs must verify the copy of the aforementioned documents with the original before accepting the same as valid. While opening a BO Account, DPs shall exercise due diligence while establishing the identity of the person to ensure the safety and integrity of the depository system.

1. For entering into account based relationship, the client may provide the following information to the intermediary:

- a) Name
- b) Aadhaar number
- c) Permanent Account Number (PAN)

2. The above information can be provided by the client electronically including through any web enabled device.

3. The intermediary shall perform verification of the client with UIDAI through biometric authentication (fingerprint or iris scanning). Mutual Funds can also perform verification of the client with UIDAI through One Time password (OTP) received on client's mobile number or on e-mail address registered with UIDAI provided, the amount invested by the client does not exceed Rs. 50,000 per financial year per Mutual Fund and payment for the same is made through electronic transfer from the client's bank account registered with that Mutual Fund.

4. PAN of such client is to be verified from the income tax website.
5. After due validation of Aadhaar number provided by the client, the intermediary (acting as KUA) shall receive the KYC information about the client from UIDAI through KSA.
6. The information downloaded from UIDAI shall be considered as sufficient information for the purpose of KYC verification. The intermediary shall upload this KYC information on the KRA system in terms of KRA Regulations.
7. In case material difference is observed either in the name (as observed in the PAN vis-a-vis Aadhaar) or photograph in Aadhaar is not clear, the intermediary shall carry out additional due diligence and maintain a record of the additional documents sought pursuant to such due diligence.
8. The records of KYC information so received shall be maintained by the intermediary as per the SEBI Act, Regulations and various circulars issued there under.

#### 36.1.4 KYC requirement for eligible Foreign Investors:

- i. SEBI has received representations regarding operational issues in the implementation of SEBI circulars No CIR/MIRSD/16/2011 dated August 22, 2011 and MIRSD/SE/Cir-21/2011 dated October 5, 2011 on know your client norms for the securities market SEBI Circulars in case of foreign investors viz. Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors. In consultation with the Stock Exchanges, Depositories and Intermediaries, certain clarifications are issued, as given in D.P. Annexure A, with respect to these investors.
- ii. Eligible foreign investors investing under Portfolio Investment Scheme ('PIS') route shall be classified as Category I, II and III as provided in D.P. Annexure B. The intermediary shall follow risk based Know Your Client norms. Accordingly, certain clarifications are hereby issued, as given in Annexure C, based on the category of these investors.

iii. Eligible foreign investors investing under PIS route shall be subject to KYC review as and when there is any change in material information / disclosure.

#### 36.1.5 Acceptance of third party address as correspondence address

- a. SEBI has no objection to a BO authorizing the capture of an address of a third party as a correspondence address, provided that the Depository Participant (DP) ensures that all prescribed 'Know Your Client' norms are fulfilled for the third party also. The DP shall obtain proof of identity and proof of address for the third party. The DP shall also ensure that customer due diligence norms as specified in Rule 9 of Prevention of Money Laundering Rules, 2005 are complied with in respect of the third party.
- b. The depository participant should further ensure that the statement of transactions and holding are sent to the BO's permanent address at least once in a year.
- c. However, the above provision shall not apply in case of PMS (Portfolio Management Services) clients.

While opening an account in the name of NRI client, the Participant should obtain copy of the RBI approval letter, if any, for acquiring securities, along with the account opening form and other necessary documents.

Participants are required to ensure that all transactions in the account are in compliance with FEMA regulations. Accordingly, Participants are advised to obtain from the NRI/FN, necessary documents evidencing general/specific approvals as may be required under FEMA regulations.

36.1.6 For HUF account, the account is opened in the name of Karta of the HUF. The HUF account should not have joint holdings. The PAN details and proof of address of HUF & Karta has to be collected.

36.1.7 Accounts opened in the name of minor can be operated by a natural guardian without any order from the court though the same is neither expressly permitted nor prohibited. For opening Minor accounts, PAN Card, Proof of Address and the photograph of the minor and Guardian has to be obtained. Photocopy of school leaving certificate / Mark sheet issued by Higher Secondary Board of respective states, ICSE, CBSE / passport of the minor / original or attested or notarized (in case of photocopy) birth certificate of the minor to ascertain the date of birth of the minor. At the time of accepting any of these documents, Participant should verify the same with the original. Account opened in the name of minor should not have joint holdings.

In the case of accounts of minor in banks, the guardian is entitled to open, operate and even close the account also. The DP account can, therefore, be operated by a natural guardian without any order from the court though the same is neither expressly permitted nor prohibited.

36.1.8 For accounts opened in the name of partners, obtain PAN Card and valid Proof of Address of all the Partners; also obtain a copy of the Partnership Deed to verify the names of Partners. Obtain an undertaking in the prescribed format from the Partners to the effect that the Partners would comply with the provisions of the Companies Act, 1956 and other applicable statutes in respect of securities of the Partnership firm held in the account opened in the names of the Partners. PAN Details and Bank account details of the Partnership firm must be collected.

36.1.9 For opening trust accounts, the following documents have to be collected: -

- (i) Requisite KYC documents, PAN Card and Bank details of the trust and the trustees.
- (ii) Notary certified true copy of the trust deed,

(iii) (Certified copy of the resolution passed by the Board of Trustees giving the names of trustees authorised by the Board of Trustees to open and operate the depository account.

(iv) In addition to these, for Registered Trusts, Certified true copy of registration certificate issued by the authority under provisions of the Bombay Public Trusts Act, 1950 or The Indian Societies Registration Act, 1860.

#### 36.1.10 Exemptions from and clarifications relating to mandatory requirement of PAN

##### Mandatory requirement of Permanent Account Number (PAN)

The demat accounts for which PAN details have not been verified are “suspended for debit” until the same is verified with the Depository Participant (DP). With effect from August 16, 2010 such PAN non-compliant demat accounts were also "suspended for credit" other than the credits arising out of automatic corporate actions. It was clarified that other credits including credits from IPO/FPO/Rights issue, off-market transactions or any secondary market transactions would not be allowed into such accounts.

##### Central and State Government and officials appointed by Courts

PAN card may not be insisted upon in case of transactions undertaken on behalf of Central Government and/or State Government and where transactions are conducted by officials appointed by Courts e.g. Official liquidator, Court receiver etc.<sup>18</sup>

However DPs, before implementing the above exemption, shall verify the veracity of the claim of the organizations by collecting sufficient documentary evidence in support of their claim for such an exemption.

Investors in Sikkim Investors residing in the state of Sikkim are exempted from the mandatory requirement of furnishing PAN card details for their demat accounts. DPs shall verify the veracity of the claim of the investors that they are residents of Sikkim, by collecting sufficient documentary evidence in support of their address.

UN entities and multilateral agencies exempt from paying taxes/ filling tax returns in India

UN entities/ multilateral agencies exempt from paying taxes/filing tax returns in India are also exempt from the mandatory requirement of submitting their PAN card details, subject to the DPs collecting documentary evidence in support of such claims.

FII/Institutional Clients

Custodians shall verify the PAN card details of institutional clients with the original PAN card and provide duly certified copies of such verified PAN details to the brokers. This requirement is applicable in respect of institutional clients, namely, FIIs, MFs, VCFs, FVCIs, Scheduled Commercial Banks, Multilateral and Bilateral Development Financial Institutions, State Industrial Development Corporations, Insurance Companies registered with IRDA and Public Financial Institution as defined under section 4A of the Companies Act, 1956.

HUF, Association of Persons (AoP), Partnership Firm, unregistered Trust, Registered Trust, Corporate Bodies, minors, etc.

The BO account shall be in the name of natural persons, PAN card details of the respective HUF, AoP, Partnership Firm, Unregistered Trust, etc shall be obtained. The PAN number of Registered Trust, Corporate Bodies and minors shall be obtained when accounts are opened in their respective names.

36.1.11 Difference in maiden name and current name of investors.

DPs can collect the PAN card proof as submitted by the account holder subject to the DPs verifying the veracity of the claim of such investors by collecting sufficient documentary evidence in support of the identity of the investors.

36.1.12 NRI/ PIOs



Citizens of India residing outside India, foreign citizens and other persons (like companies/ trusts/ firms) having no office of their own in India may obtain PAN card based on the copy of their passport as ID proof and a copy of passport/ bank account in the country of residence as address proof, based on the Directorate of Income Tax (Systems) guidelines.

#### Simplification of Demat account opening process

i. SEBI has taken a number of steps in the recent past to simplify the Account opening and KYC process in the securities markets. In continuation of the efforts in the same direction, it has now been decided in consultation with both the Depositories and Associations of stock brokers and Depository

Participants to further simplify and rationalize the demat account opening process.

ii. The existing Beneficial Owner-Depository Participant Agreements shall be replaced with a common document “Rights and Obligations of the Beneficial Owner and Depository Participant”. The document annexed herewith shall be mandatory and binding on all the existing and new clients and depository participants. This will harmonize the account opening process for trading as well as demat account. This will also rationalise the number of signatures by the investor, which he is required to affix at present on a number of pages.

iii. The Depository Participant shall provide a copy of Rights and Obligations Document to the beneficial owner and shall take an acknowledgement of the same. They shall ensure that any clause in any voluntary document neither dilutes the responsibility of the depository participant nor it shall be in conflict with any of the clauses in this Document, Rules, Bye-laws, Regulations, Notices, Guidelines and Circulars issued by SEBI and the Depositories from time to time. Any such clause introduced in the existing as well as new documents shall stand null and void.

#### 36.1.13 Guidelines in respect of account opening in case of Body-Corporate

Procedure for opening account of a Body-Corporate:

Participants shall obtain the following documents at the time of account opening:

- (a) Memorandum & Articles of Association, Certificate of Incorporation board resolution for opening and operating depository account and the list of authorised signatories along with their specimen signatures and photographs etc.
- (b) Proof of Address of the corporate evidenced by the document registered with Registrar of Companies (ROC) or an acknowledged copy of Income Tax Return or Bank Statement or Leave and License agreement/Agreement for sale or telephone bill (not more than two months old) or electricity bill (not more than two months old) in the name of body-corporate.
- (c) Copy of the balance sheets for the last 2 financial years (to be submitted every year).
- (d) Names of authorised signatories, designation along-with their specimen signatures and photographs, duly verified by the Managing Director or Company Secretary.
- (e) Copy of latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/Whole time director/MD (to be submitted every year).
- (f) Photograph, POI, POA, PAN and DIN numbers of whole time directors/two directors in charge of day to day operations.
- (g) Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly.
- (h) Copy of the Board Resolution for investment in securities market.

An authorised official of the Participant should verify the proof of address with the original documents and put his/her signature on them with remarks "verified with original" before proceeding to open the account.

PAN, address and bank details of the body-corporate should be captured after due verification.

(2) Additional requirement with respect to Foreign Corporate Bodies:

(a) Participants are advised to obtain photocopies of Proof of Address in respect of foreign address in case of FII, Foreign Corporate Bodies, Foreign Banks, Overseas Corporate Bodies etc. (referred as foreign entities) and verify the same with originals. In case these foreign entities also have an Indian address, Participants are advised to obtain the photocopies of Proof of Address of local address and verify the same with originals. Further, in case if these entities have submitted only Proof of Address as foreign address, in such a situation, Participants may capture the foreign address in both local and foreign address fields given in the DPM System.

(b) If Participants find it infeasible to verify the original KYC documents (foreign address of these foreign entities) and PAN card, in such a situation it is clarified that:

- (i) The KYC documents and PAN should be duly signed by the authorised signatories; and
- (ii) Attested by the Indian Embassy / Consulate General of the country where the registered office of the foreign entity is situated and
- (iii) The attestation is to the effect that it has been verified with the originals.

Participants should open the depository account or accept the PAN card only after it is satisfied with the authenticity of the documents (Proof of Address and PAN card).

(c) As regards proof of address of FIIs/sub-accounts, a copy of the Power of Attorney given by the FIIs/FII sub-accounts to the Custodians (which are duly notarized and/or apostilled or consularised) that gives the registered address of the FIIs/sub-accounts can be accepted as proof of address.

(d) U.N. entities/multilateral agencies which are exempt from paying taxes/filing tax returns in India are exempted from the mandatory requirement of PAN. The exemption, however, would be subject to the Participants collecting documentary evidence in support of claim of such entities/agencies. After the Participants are satisfied that such entities are exempt from paying taxes/filing tax returns in India, Participants are advised to capture the description "EXEMPTCATG" under the PAN field and enable the PAN flag in DPM System.

- (e) Participants need not enter into Participant-Client agreement provided:
  - (i) FIIs are registered with SEBI and have entered into an agreement with the Participant either directly or through their power of attorney holders in accordance with the provisions of sub-regulation (1) of regulation 16 of the SEBI (Foreign Institutional Investors) Regulations, 1995; and
  - (ii) Such agreement gives the Participant an authority to act on behalf of the FIIs for availing the services of the Depository; and
  - (iii) Such agreement has been filed with SEBI;
  - (iv) International Multilateral Agency, who has entered into an agreement with the Participant under regulation 17 of the SEBI (Custodians of Securities) Regulations 1996, and such agreement states that the Custodian will also act as a Participant and all provision pertaining to Participant shall be applicable; then such Participant need not enter into an agreement as per Annexure B of the Bye Laws.
- (f) Participants shall ensure that in case of foreign entities, all transactions in the account are in compliance with FEMA Regulations. Accordingly, Participants are advised to obtain from such foreign entities necessary documents evidencing general/specific approvals as may be required under FEMA Regulations.
- (g) Obtain a declaration from the foreign entity that it has complied and will continue to comply with FEMA Regulations.

#### 36.1.14 Guidelines in respect of account opening in case of “Nidhi Company”

“Nidhi” means a company which has been incorporated as a Nidhi with the object of cultivating the habit of thrift and savings amongst its members, receiving deposits from, and lending to, its members only, for their mutual benefit and which complies with the rules made by the Central Government for regulation of such class of companies.

Declaration of Nidhis – The Central Government, on receipt of application of a public company for declaring it as Nidhi and on being satisfied that the company meets the requirements under these rules, shall notify the company as a Nidhi in the official Gazette:

Bank should obtain a copy of declaration of Nidhi Company about the Gazette notifications while opening the account.

37. **Annexure 7**

37.1 Centralised Monitoring of transactions by AML Department:

*Disclaimer: This is an abridged version after excluding confidential part.*