POLICY ON

KNOW YOUR CUSTOMER (KYC),

ANTI MONEY LAUNDERING (AML) MEASURES

AND

COMBATING FINANCING OF TERRORISM

(CFT)

Version 2021

Table of Contents

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, 2021.

2. Objective

The objective of the Policy is:

2.1 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.

2.2 To prevent the Bank from being used intentionally or unintentionally by criminal elements for money laundering or terrorist financing activities.

2.3 To put a proper control mechanism for detecting and reporting suspicious transactions under the statutory and regulatory provisions.

2.4 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

2.5 To ensure compliance with guidelines/instructions issued by the regulators, including FIU-IND and RBI.

3. Applicability

3.1 RBI Master Direction – Know Your Customer (KYC) Direction, 2016 dated February 25, 2016, and updated as of May 10, 2021, 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 25 per cent 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 15 per cent of capital or profits of the partnership.

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more

juridical person, has/have ownership of/ 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 15% 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 that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

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 nominated by the Bank, responsible for furnishing information as per rule 8 of the 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 subrule (5) 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.

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 they are consistent with the customers' profile and source of funds.

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 is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

4.2.14 "Wire transfer" means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

4.2.15 "Domestic and cross-border wire transfer": When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or

'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

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.

6.2 The assessment process should consider all the relevant risk factors before determining the overall risk level and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance

of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Bank from time to time.

6.3 The risk assessment by the Bank shall be appropriately documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc., of the Bank. Further, the periodicity of the risk assessment exercise shall be determined by the Board of the Bank, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

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)

Bank shall develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the Bank and including the following aspects of customer relationship in the Bank.

8.1 No account is opened or maintained in anonymous or fictitious / benami name.

8.2 Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Bank in categorizing the customers into low, medium and high risk ones, as detailed in Section 9 and 10.

8.3 While opening an account and during the periodic updation, documents and other information to be collected from different categories of customers are detailed in Section 20 and Annexure 5.

8.4 Bank will not open an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/ or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. Bank may also consider closing an existing account under similar circumstances.

8.5 Optional / Additional information is obtained with the explicit consent of the customer after the account is opened.

8.6 No transaction or account based relationship is undertaken without following the CDD procedure.

8.7 Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking.

8.8 Bank shall have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

8.9 Bank shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level. Thus, if an existing KYC compliant customer desires to open another account with our bank, there shall be no need for a fresh CDD exercise.

8.10 CDD procedure is followed for all the joint account holders, while opening joint account.

8.11 Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

8.12 Where an equivalent e-document is obtained from the customer, bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

8.13 Adoption of customer acceptance policy and its implementation shall not become too restrictive, which result in denial of banking facility to the members of the general public, especially to those, who are financially or socially disadvantaged.

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 Networth) 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, such as:

- Salaried employees
- People belonging to lower economic strata of the society
- Government Departments
- Government owned companies
- Regulatory and Statutory bodies, etc.

For the above category, the KYC requirements of proper identification and verification of proof of address would suffice.

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.

9.2.2 An indicative list of Medium Risk Customers is as under:

- Gas Dealers
- Car/boat/plane dealers
- Electronics (wholesale)
- Travel agency
- Telemarketers
- Telecommunication service providers
- Pawnshops
- Auctioneers
- Restaurants, Retail shops, Movie theatres, etc.
- Sole practitioners
- Notaries
- Accountants
- Blind
- Purdanashin

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. An indicative list of High Risk customers is as under:

- Trusts, charities, NGOs and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'.

- Accounts under Foreign Contribution Regulation Act.

- Politically Exposed Persons (PEPs).

- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.

- Those with dubious reputation as per public information available.

- Accounts of non-face-to-face customers.

- High Net worth Individuals*

- Non-Resident customers.

- Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewelers.

* Parameters for defining High Net worth Individuals based on account balance:

Customers with any of the following:

1) Average balance threshold defined internally.

2) Enjoying Fund based limits/term loans exceeding threshold defined internally.

The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Branch/Office.

Branches shall prepare a Risk profile of each customer and apply enhanced due diligence measures on High Risk customers. IBA has provided an indicative list of High/Medium Risk Products, Services, Geographies,

Locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure 2 to 4).

10. Customer Risk Categorisation

10.1 As per IBA Working Group guidelines, Bank may choose to carry out either manual classification or automatic classification or a combination of both. Similarly for selecting parameters, Bank may select the parameters based on the available data. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter.

10.2 Bank has adopted combination of manual and automatic classification. Based on the availability of data, Bank shall finalise parameters which are available in the system and the same shall be reviewed annually. System shall assign provisional risk categorization based on the system provided parameters. AML team shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy.

10.3 Branches/Operations shall prepare a profile for all Customers based on risk categorization.

10.4 The Customer profile may contain information relating to Customer's identity, social/financial status, nature of business activity, information about his client's business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. Risk categorization shall be done based on selected parameters and assigning suitable risk category.

10.5 Risk Parameters

10.6 The first step in process of risk categorization is selection of parameters, which would determine customer risk.

10.7 IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used, to determine the profile and risk category of Customers:

1. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
2. Business Segment : Retail, Corporate etc.
3. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national.
4. Product Subscription: Salary account, NRI products etc.
5. Economic Profile: HNI, Public Ltd. Company etc.
6. Account Status: Active, inoperative, dormant.
7. Account Vintage: Less than six months old etc.
8. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.
9. Suspicious Transaction Report (STR) filed for the customer.
10. AML alerts.

10.8 Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc. can also be used in addition of the above parameters. Bank shall adopt all or majority of these parameters based on availability of data.

10.9 Risk rating of Customers:

10.10 Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of origin, sources of funds and client profile etc.

A. An Illustrative list of Low/Medium/High Risk Customers, Products, Services, Geographies, etc., based on the recommendations of IBA Working Group on Risk Based Transaction Monitoring is detailed in Annexure1, 2, 3 and 4 of this Note.

B. Risk rating based on the Deposits/account balance: As per the threshold defined internally.

Above categorization of the Customer shall be based on all accounts linked to Customer ID irrespective of constitution of account like Joint account, Partnership account etc. However accounts linked to Customer ID where customers do not have any stake in Business/activity need not be clubbed for the above purpose.

C. Risk Categorization of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

- Unusual transaction/behavior (given as Annexure 4 – Monitoring of Customer Risk Categorisation (CRC).
- Submitted Suspicious Transaction Reports (STR) for Customer.
- Submitted Cash Transaction Report (CTR).
- Frequent Cheque returns.

D. Risk Categorisation of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen

parameters, highest risk grade will be assigned as overall Risk for the customer.

Risk categorization of Customers undertaken by the Bank:

Based on the policy/guidance notes of RBI/IBA and also the methodology of Customer Risk Categorisation provided by IRM Department (as detailed under points A, B, C & D above), risk rating has been assigned taking into account the following parameters available in CBS system :

- Customer type.
- Customer profession.
- Type of business.
- Product code.
- Account status
- Account vintage.
- Average balance in deposits in SB/Current/Term Deposit accounts.

Note: While assigning risk category, the average balance criteria will be applied after applying conditions related to customer type, business category, product, STR status etc.

10.11 All customer profiles/accounts of NRIs, HNIs, PEPs, NGOs, Trusts, Co-operative Societies, HUF, Exporters, and Importers shall be invariably categorised as High Risk, irrespective of the lower risk category (low/medium) allotted under other parameters in the Matrix like customer profession, type of business, product code, account status, account vintage and balance in the account.

10.12 As per RBI directions, the parameters used for categorising the risk profile of customers should include those named in complaints (from legal enforcement

authorities)/frauds. As the system will not identify the customers/accounts named in complaints (from legal enforcement authorities)/frauds, this parameter has not been included in the Risk Categorisation Matrix. Branches/Operation are advised to categorise such customers/ accounts under "High Risk" category as and when complaints (from legal enforcement authorities) are received or fraud is reported against the customer/account holder.

10.13 Accounts of dealers in jewellery, gold/silver/bullions, diamonds and other precious metals/stones shall be categorised under High Risk.

10.14 The Roles and Responsibilities of Authorities for Customer Risk Categorisation:

10.14.1 Roles and responsibilities of Branches/Central Operations:

a. Branches/Operations may also apply additional alert indicators to address specific risks faced by them.
b. Shall attend/follow-up audit observations/remarks.

10.15 AML Team, H.O:

a. AML team shall review Customer risk categorization based on the risk categorization generated by the system, every six months, as on 15th of May and November every year.
b. Shall submit periodical reports on implementation/review of risk categorisation to Compliance team.
c. Shall review and provide necessary recommendations/directions to strengthen adherence of KYC/AML guidelines.
d. Shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

10.16 Monitoring/Review of Customer Risk Categorisation (CRC):

10.16.1 AML Team shall carry out a review of risk categorization of customers at a periodicity of not less than once in six months i.e., as on 15th of May and November every year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.

10.16.2 Wherever there is suspicion at branch level that a Customer is above low risk, branches should carry out customer due diligence (CDD).

10.16.3 While monitoring of transactions, AML team / branches shall arrive at a conclusion whether the transaction is suspicious or not, based on objective parameters for enhanced due diligence. Some of the objective parameters for enhanced due diligence could be:

- Customer locations.
- Financial Status.
- Nature of business.
- Purpose of transaction.

Monitoring of Customer Risk Categorisation (CRC) – given as Annexure 4 to this Note.

11. 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).

11.1 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.).

11.2 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.

12. Customer Due Diligence requirements while opening accounts

12.1 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.

12.2 Accounts of individuals:

12.2.1 For undertaking Customer Due Diligence (CDD), 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:

12.2.2 The Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank; or

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

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

12.2.3 The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

12.2.4 One recent photograph

12.2.5 Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank.

12.2.6 Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank, such bank shall carry out authentication of the customer's Aadhaar number using e-KYC

authentication facility provided by the Unique Identification Authority of India.

Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.

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

iii) An equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

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.

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

12.2.7 Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, 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 e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

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

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

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

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

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

12.2.13 In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain.

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

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

12.3.2 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.

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

12.3.4 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.

12.3.5 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.

12.3.6 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.

12.3.7 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.

12.3.8 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.

12.4 Bank may undertake Video based Customer Identification Process (V-CIP) to carry out

12.4.1 CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 16, apart from undertaking CDD of the proprietor.

12.4.2 Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 14.

12.4.3 Updation/Periodic updation of KYC for eligible customers. Bank opting to undertake V-CIP, shall adhere to the following minimum standards:

12.5 (A) V-CIP Infrastructure

12.5.1 The Bank should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Bank and the V-CIP connection and interaction shall

necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

12.5.2 The Bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

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

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

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

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

12.5.7 The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and

end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

12.6 (B) V-CIP Procedure

12.6.1 Bank shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Bank specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

12.6.2 If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

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

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

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

12.6.6 The authorised official of the Bank performing the V-CIP shall record audiovideo as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

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

12.6.7 Bank shall ensure to redact or blackout the Aadhaar number

12.6.8 In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

12.6.9 Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Bank shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification

information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Bank shall ensure that no incremental risk is added due to this.

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

12.6.11 Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

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

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

12.6.14 Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Bank shall maintain the details of the BC assisting the customer, where services of BCs are

utilized. The ultimate responsibility for customer due diligence will be with the bank.

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

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

12.7 (C) V-CIP Records and Data Management

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

12.7.2 The activity log along with the credentials of the official performing the VCIP shall be preserved.

12.8 Introduction of accounts:

12.8.1 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.

12.9 Accounts of married woman:

12.9.1 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.

12.9.2 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.

12.10 Small Accounts:

12.10.1 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.

12.10.2 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.

13. Basic Savings Bank Deposit Accounts

13.1 As per RBI guidelines, the Basic Savings Bank Deposit Account should be considered a normal banking service available to all.

13.2 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.

13.3 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.

13.4 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.

13.5 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.

13.6 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:

13.6.1 Records of the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

13.6.2 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;

13.6.3 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;

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

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

14. Account opened using OTP based e-KYC, in non-face-to-face mode

The bank may open accounts using OTP based e-KYC in non-face-to-face mode subject to the following conditions:

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

14.2 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 (14.5) below is complete.

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

14.4 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.

14.5 Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which full KYC shall be carried out.

14.6 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.

14.7 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 non-face-to-face mode with any other Regulated Entity. Further, while uploading KYC information to CKYCR, the bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

14.8 The 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.

14.9 Accounts of non-face-to-face customers (Other than Aadhaar OTP based on-boarding): Bank shall ensure that the first payment is to be effected through the customer's KYC-complied account with another bank, for enhanced due diligence of nonface- to-face customers.

14.10 Accounts of Foreign students studying in India:

Considering that foreign students 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:-

14.10.1 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.

14.10.2 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.

14.10.3 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.

14.10.4 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.

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

14.11 Accounts of Politically Exposed Persons (PEPs) resident outside India

14.11.1 Politically Exposed Persons 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. 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.

14.11.2 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 branch head in branches headed by Scale IV and above. For all other branches, the decision is to be taken by the executive overseeing respective Regional Office.

14.11.3 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.

14.11.4 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.

15. Accounts of persons other than individuals:

15.1 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.

16. CDD Measures for Sole Proprietary firms

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

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:

16.1.1 Registration certificate

16.1.2 Certificate / License issued by the municipal authorities under Shop and Establishment Act.

16.1.3 Sales and income tax returns.

16.1.4 CST / VAT / GST certificate (provisional / final).

16.1.5 Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.

16.1.6 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.

16.1.7 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.

16.1.8 Utility bills such as electricity, water, and landline telephone bills. In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank may, at their discretion, accept only one of those documents as proof of business / activity.

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

17. CDD Measures for Legal Entities

17.1 For opening an account of a company, certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

i. Certificate of incorporation;
ii. Memorandum and Articles of Association;
iii. Permanent Account Number of the company;
iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
v. Documents, as specified in Section 12, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

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

i. Registration certificate;
ii. Partnership deed;
iii. Permanent Account Number of the partnership firm; and
iv. Documents, as specified in Section 12, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

17.3 For opening an account of a trust, certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

i. Registration certificate;
ii. Trust deed;
iii. Permanent Account Number or Form No.60 of the trust; and
iv. Documents, as specified in Section 12, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

17.4 For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

i. Resolution of the managing body of such association or body of individuals;
ii. Permanent account number or Form No.60 of the unincorporated association or a body of individuals;

iii. Power of attorney granted to transact on its behalf;

iv. Documents, as specified in Section 12, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and

v. such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

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

Explanation: Term 'body of individuals' includes societies.

17.5 For opening accounts of juridical persons, not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-document thereof shall be obtained:

i. Document showing name of the person authorised to act on behalf of the entity;

ii. Documents, as specified in Section 12, of the person holding an attorney to transact on its behalf and

iii. Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

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

i. Identification information as mentioned under Section 12 in respect of the Karta and Major Coparceners,

ii. Declaration of HUF and its Karta,

iii. Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.

iv. The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

18. Identification of Beneficial Owner

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

18.1.1 Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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

19. On-going Due Diligence

19.1 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.

19.2 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.

20. Periodic updation of KYC

Bank shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

20.1 Individual Customers:

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

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

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

20.2 Customers other than individuals:

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

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

20.3 Additional measures: In addition to the above, Bank shall ensure that,

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

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

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

20.3.4 In case of existing business relationship which is not KYC compliant, Bank shall temporarily cease operations in the account. However, before temporarily ceasing operations for an account, the Bank shall give the client two notices of 10 days each and within 30 days period the account should be made KYC compliant otherwise operations in the account shall be frozen. The account holders shall have the option, to revive their accounts by submitting the KYC documents. However, keeping in view the COVID related restrictions in various parts of the country, all offices are

being advised that for the customer accounts where periodic KYC updating is due/pending, no punitive restriction on operations of customer account(s) shall be imposed till 31.12.2021 unless warranted due to any other reason or under instructions of any regulator/enforcement agency/court of law, etc. Field functionaries are advised to request Customers to get their KYC updated during the period.

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

20.4.1 Provided that before temporarily ceasing operations for an account, the Bank shall give the client an accessible notice and a reasonable opportunity to be heard.

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

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

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

21. Miscellaneous

21.1 Operation of Bank Accounts & Money Mules

21.1.1 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.

21.1.2 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.

21.2 Simplified norms for Self Help Groups (SHGs):

21.2.1 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:

21.2.2 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.

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

21.3 Walk-in Customers

21.3.1 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.

21.3.2 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.

22. Issue of Demand Drafts, etc., for more than Rs. 50,000/-

22.1 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.

22.2 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.

22.3 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.

23. Unique Customer Identification Code

23.1 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.

23.2 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.

24. Monitoring of Transactions:

24.1 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:

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

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

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

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

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

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

24.3 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.

24.4 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.

24.5 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.

24.6 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.

24.7 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 serious 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.

24.8 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.

24.9 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.

25. Risk Management:

25.1 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.

25.2 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.

25.3 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.

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

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

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

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

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

25.4.5 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.

25.4.6 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.

25.4.7 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:

25.4.8 Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, shall be categorised as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc.

25.4.9 Customers who are likely to pose a higher than average risk shall be categorised as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, shall be categorised as high risk.

25.4.10 Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of business relationship.

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

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

25.5.1 Business development and Planning Section-

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

25.5.3 AML/CFT Centralised Unit

25.5.4 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.

25.5.5 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.

25.6 CORRESPONDENT BANKING AND SHELL BANK:

25.6.1 Correspondent Banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash / funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Bank shall take the following precautions while entering into a correspondent banking relationship:

25.6.2 Bank shall gather sufficient information to fully understand the nature of the business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank‟s home country.

25.6.3 Such relationships may be established only with the approval of the Board or by a committee headed by the MD & CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.

25.6.4 The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.

25.6.5 In the case of payable-through-accounts, Bank shall satisfy that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.

25.6.6 Bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

25.6.7 Bank shall be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of Financial Action Task Force (FATF) Recommendations.

25.6.8 Bank shall ensure that its respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

25.6.9 Bank shall not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group).

25.6.10 Bank shall not permit its accounts to be used by shell banks.

25.7 WIRE TRANSFERS:

25.7.1 Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not

involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

25.7.2 The salient features of a wire transfer transaction are as under:

25.7.3 Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

25.7.4 Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

25.7.5 Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.

25.7.6 The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

25.7.7 Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law

enforcement and / or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary.

25.7.8 The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits.

Accordingly, Bank shall ensure that all wire transfers are accompanied by the following information.

25.7.9 Cross-border wire transfers

25.7.10 All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

25.7.11 Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

25.7.12 Domestic wire transfers

25.7.13 Information accompanying all domestic wire transfers of Rs. 50,000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name,

address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

25.7.14 If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank shall insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.

25.7.15 When a credit or debit card is used to effect money transfer, necessary information as above should be included in the message.

Exemptions

25.7.16 Inter-bank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

25.7.17 Role of Ordering, Intermediary and Beneficiary Banks

25.8 Ordering Bank

25.8.1 An Ordering Bank is the one that originates a wire transfer as per the order placed by its customer. As Ordering Bank, the Bank shall ensure that qualifying wire transfers contain complete originator information. The Bank shall also verify and preserve the information at least for a period of five years.

25.9 Intermediary Bank

25.9.1 For both cross-border and domestic wire transfers, Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) as the receiving Intermediary Bank, of all the information received from the Ordering Bank.

25.10 Beneficiary Bank

25.10.1A Beneficiary Bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. As Beneficiary Bank, the Bank shall also take up the matter with the Ordering Bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

26. Record Management

26.1 PML Act and Rules cast certain obligations on the banks with regard to maintenance, preservation and reporting of customer account information. Bank shall take all steps considered necessary to ensure compliance with the requirements of the Act and Rules ibid.

26.2 Maintenance of records of transactions

26.2.1 Bank shall maintain all necessary information in respect of transactions prescribed under Rule 3 of PML Rules, 2005 so as to permit reconstruction of individual transactions, including the following information:

(a) the nature of the transactions;

(b) the amount of the transaction and the currency in which it was denominated;

(c) the date on which the transaction was conducted; and

(d) the parties to the transaction.

26.3 Preservation of Records

26.3.1 Bank shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

26.3.2 Bank shall maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

26.3.3 Bank shall ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving

licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification records and transaction data shall be made available to the competent authorities upon request.

26.3.4 Bank shall maintain records of the identity of clients, and records in respect of transactions with its clients referred to in Rule 3, in hard or soft format.

27. Combating Financing of Terrorism (CFT)

27.1.1 The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC):

27.1.2 The ISIL (Daesh) & Al-Qaida Sanctions List includes names of individuals, groups, undertakings and entities associated with the ISIL (Daesh) /Al-Qaida. The updated ISIL (Daesh) /Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

27.1.3 The 1988 Sanctions List consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban, which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

27.1.4 The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Bank shall take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967. Branches are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts.

27.1.5 Branches are required to ensure that the names/s of the proposed customer does not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account. AML/CFT Centralised Unit, Head Office will also cross check the details of all existing accounts with the updated list, on a regular basis. If the particulars of any of the account/s have resemblance with those appearing in the list, branches have to verify transactions carried out in such accounts and report those accounts to RBI/Financial Intelligence Unit-INDIA apart from advising Ministry of Home Affairs as required under UAPA notification dated Mar 14, 2019.

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

27.2.1 The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be

engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

27.2.2 Bank shall strictly follow the procedure laid down in the UAPA Order dated March 14, 2019 (Annexure VI to this note) and ensure meticulous compliance to the Order issued by the Government.

27.3 Jurisdictions that do not or insufficiently apply the FATF Recommendations

27.3.1 Bank shall take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the Financial Action Task Force (FATF) Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time,

27.3.2 Bank shall also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. Bank shall also give special attention 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.

27.3.3 Bank shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible

lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to Reserve Bank/other relevant authorities, on request.

28. Reporting Requirements

28.1 Reporting to Financial Intelligence Unit-India as per the regulatory requirements.

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

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

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

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

28.2.4 Explanation: Banks shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at

http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

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

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

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

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

29. General Guidelines:

29.1 Confidentiality of customer information:

29.1.1 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.

29.2 Secrecy Obligations and Sharing of Information:

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

29.2.2 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.

29.3 Hiring of Employees:

29.3.1 KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank shall put in place adequate screening mechanism as an integral part of its personnel recruitment / hiring process.

29.4 Employee Training:

29.4.1 Bank shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers.

29.4.2 The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Bank, regulation and related issues shall be ensured.

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

29.5.1 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.

29.5.2 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.

29.5.3 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.

29.5.4 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.

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

29.6 Designated Director on the Board of the Bank:

29.6.1 Bank has nominated the Managing Director of the Bank as the Designated Director on the Board of the Bank, as required under the provisions of the PML Rules, 2005,

to ensure compliance with the obligations under the Act and Rules. The Designated Director shall oversee the compliance position of AML norms in the Bank.

29.6.2 If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may -

(a) issue a warning in writing; or

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

It shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions.

29.7 Principal Officer:

29.7.1 Bank has appointed a Principal Officer. The Principal Officer shall be independent and report directly to the senior management or to the Board of Directors.

29.7.2 Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

29.7.3 The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

29.7.4 The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by Non-Profit Organisations of value more than Rupees ten lakh or its equivalent in foreign currency to FIU-IND.

29.7.5 The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.

29.7.6 The Principal Officer under PMLA Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

29.8 Need for photographs and address confirmation:

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

29.8.2 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.

29.8.3 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.

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

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

29.9 Sale of third party products:

29.9.1 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.

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

29.10.1 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.

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

29.11.1 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 No. S.O. 3183(E) dated November 26, 2015.

29.11.2 In terms of provision of Rule 9(1A) of PML Rules, the Bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

29.11.3 Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

29.11.4 The Bank is required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR.

29.11.5 The Bank shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

29.11.6 Once KYC Identifier is generated by CKYCR, Bank shall ensure that the same is communicated to the individual/LE as the case may be.

29.11.7 In order to ensure that all KYC records are incrementally uploaded on to CKYCR, REs shall upload/update the KYC data pertaining to accounts of individual customers and Bank opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation or earlier, when the updated KYC information is obtained/received from the customer.

29.11.8 The Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

29.11.9 Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Bank, with an explicit consent to download records from CKYCR, then Bank shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

(i) there is a change in the information of the customer as existing in the records of CKYCR;

(ii) the current 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 client.

29.12 Period for presenting payment instruments

29.12.1 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.

29.13 Collection of Account Payee Cheques

29.13.1 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.

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

29.14.1 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).

29.14.2 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.

29.14.3As 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.

30. Annexure 1

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

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

31. Annexure 2

31.1 High / Medium Risk Products and Services

31.1.1 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.

31.2 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.

32. Annexure 3

32.1 High / Medium Geographic risk

32.1.1 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.

32.1.2 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.)

32.1.3 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.

32.2 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)

3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (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.

33. Annexure 4

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

34. Annexure 5

34.1 List of document to be collected for Account opening – Details

34.1.1 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 therof 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.

34.2 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.

34.3 Accounts of Partnership Firms

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

Features to 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/Auhtorised 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.

34.4 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.

34.5 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 Kartha

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 Kartha and Co-parceners, who have attained majority.

34.6 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.

34.7 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)

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

34.8.1 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.

34.8.2 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 consists 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.

34.9 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 panchayaths, 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.

34.10 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 MSS, 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.

34.11 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.

34.12 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, T. Nadu, Karnataka, Maharashtra. Etc.).

34.13 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

34.14 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.

34.15 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

34.16 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)

34.17 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.

Bank will not entertain opening of accounts for Oral Wakfs.

The following documents need to be obtained to open Wakfs account. A certified copy of

1. Registration certificate with the Wakf Board by Mutawalli.
2. Wakfs Deed / Wakfnamah by Mutawalli.
3. Letter from Mutawalli to open the account.
4. Any Officially valid document containing details of identity and address, one recent photograph and PAN or Form 60 of the authorised signatories
5. Copy of PAN of the Wakf
6. Address proof, in case it is not part of the Wakf Deed/Wakf namah / Registration Certificate.
7. Proof of tax exemption in case it wants to open a SB a/c or else Bank can open only Current account.

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.

34.18 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;

34.19 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.

34.20 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.

34.21 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.

34.22 Accounts of Politically Exposed Persons (PEPs) resident outside India

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

Branch should

(a) Gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

(b) Gather and verify the identity of the PEP and seek information about the sources of funds / accounts of family members and close relatives before accepting the PEP as a customer.

(c) The decision to open an account for a PEP should be taken at a senior level, i.e. Regional Head, which is spelt out in Customer Acceptance Policy.

(d) All such accounts are to be subjected to enhanced monitoring on an ongoing basis (*). The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

(e) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, Branch should obtain Regional Head's approval to continue the business relationship and subject the account to the Customer Due Diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

Further, Branch should have appropriate ongoing risk management procedures 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.

(*) PEPs in our Bank context would include foreigners having the above assignments in India.

34.23 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.

35. Annexure 6

35.1 Depository Accounts

35.1.1 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)(AADHAR)

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.

35.1.2 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) and c)

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

35.1.3 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.

35.1.4 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.

35.1.5 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.

35.1.6 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.

35.1.7 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.

35.1.8 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.

35.1.9 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.

35.1.10 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.18

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.

FIIs/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.

35.1.11 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.

35.1.12NRI/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

35.1.13 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 apostiled 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. Annexure 7

36.1 Centralised Monitoring of transactions by AML Desk: As per internal and regulatory guidelines.

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