KYC / AML Policy – 2025-26

Previous KYC/AML policy of our bank is as per RBI guidelines and was approved in the Board meeting dated 28.04.2023. Earlier the said policy was changed in the Board of Directors meeting on 10.11.2023 as per Master Direction of Reserve Bank dated 17.10.2023. Also, according to Master Direction of Reserve Bank dated 04.01.2024, the Board of Directors was informed that it is necessary to change the concept of Politically Exposed Persons (PEP's) and add a new explanation. The said policy is changed in the Board of Directors meeting on 11.11.2024 as per Master Direction of Reserve Bank dated 06.11.2024. & also as per FIU IND guidelines regarding Wildlife Trafficking RFI updation in transaction monitoring & RBI advisory circular regarding use of money mule accounts for cyber enabled frauds said policy is changed in the Board of Directors meeting on 13.12.2024. Now, for year 2025-26 review of policy has been taken in the Board of Directors meeting on 09.05.2025.

1. **Introduction -** Prevention of Money Laundering Act 2002 is applicable throughout India. According to RBI's Master Direction dtd. 28.04.2023 and according to this act's chapter - 1 (Chapter I: Preliminary) the following definations are given:

2. Definitions

In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005: **i.** 2"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

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

iii. 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.

iv. Beneficial Owner (BO)

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

1. 4“Controlling ownership interest” means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

2. “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their 5 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 percent of capital or profits of the partnership.~~

Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership. **(Amended 10/11/2023 BOD)**

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 percent of the property or capital or profits of the unincorporated association or body of individuals. Explanation: Term ‘body of individuals’ includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. 5Where the customer is **a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or

more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. 6 “Certified Copy” - Obtaining a certified copy by the RE shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act. 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, certified by any one of the following, may be obtained:

• authorised officials of overseas branches of Scheduled Commercial Banks registered in India,

• branches of overseas banks with whom Indian banks have relationships,

• Notary Public abroad,

• Court Magistrate,

• Judge,

• Indian Embassy/Consulate General in the country where the non-resident customer resides.

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

vii. “Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks. Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013. **viii.** 7"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the Act.

ix. 8"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).

x. 9"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 7 per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

xi. 10"Group" – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

xii. 11"Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.

xiii. 12"Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

xiv. "Officially Valid Document" (OVD) means the passport, the driving licence, 13proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State

Government and letter issued by the National Population Register containing details of name and address. Provided that,

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

b. 14where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

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

ii. property or Municipal tax receipt;

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

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial 8 banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

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

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

xv. 15"Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

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

a. an individual,

b. a Hindu undivided family,

c. a company,

d. a firm,

e. an association of persons or a body of individuals, whether incorporated or not,

f. every artificial juridical person, not falling within any one of the above persons (a to e), and

g. any agency, office or branch owned or controlled by any of the above persons (a to f).

~~**xvii.** 16"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.~~

(Deleted 12/01/2024 as per MD amendment 04/01/2024)

xviii. "Principal Officer" means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules. 9

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

xx. A 'Small Account' means a savings account which is opened in terms of sub-rule (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 23. **(Amended 10/11/2023 BOD)**

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

a. opening of an account;

b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c. the use of a safety deposit box or any other form of safe deposit;

d. entering into any fiduciary relationship;

e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f. establishing or creating a legal person or legal arrangement.

(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange 10 information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. 17Correspondent Banking: Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable through accounts and foreign exchange services.

iii. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

v. 23"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. **Explanation –** The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

(c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification. **(Amended 10/11/2023 BOD)**

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

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

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

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

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

~~**xi.** "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.~~

"On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that those are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds / wealth. **(Amended 10/11/2023 BOD)**

xii. [19]Payable-through accounts: The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf. 11

xiii. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank. **xiv**. "Regulated Entities" (REs) means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)

d. Asset Reconstruction Companies (ARCs) **(Amended 10/11/2023 BOD)**

e. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

f. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xv. 20Shell Bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xvi. [21]"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 RE 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 audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

xvii. "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 12 bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

xviii. "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.

(c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the 22Aadhaar (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.

1.1. Banks are required to formulate a policy as per the guidelines of "Know Your Customer" issued by the Reserve Bank of India and the provisions of the Prevention of Money Laundering Act 2002 and implement it.

1.2. The Reserve Bank of India has issued these instructions as per the recommendations made by 'Financial Action Task Force (FATF) and international cooperative organizations to effectively curb the activities of terrorists.

1.3. According to this policy, for KYC and AML of our bank instructions and policies given by Reserve Bank of India and Govt. of India - FIU IND from time to time should be followed and implemented the same in the policies.

1.4. To prevent crime, anti-social tendencies and anti-national economic activities by following this policy.

Master Direction Know your customer (KYC) Direction 2016 circular of Reserve Bank Updated As on 28 April 2023 has covered the following matters. For more information, the said circular is attached.

3. Identification of Policy-

Money Laundering is a process by which individuals with a criminal background attempt to conceal the ownership and source of proceeds from criminal activities. Because of this, they try to get relief / freedom from legal action, arrest and crime. Attempts to legitimize such wealth remain a major problem worldwide. To reduce such crimes, strict laws and heavy penalties are being implemented in many countries.

This type of law has been passed by the legislature of our country as Prevention of Money Laundering Act 2002 (PMLA) in 2002

The purpose of such a policy is mainly to prevent banks from being used to launder the money of this type of crime. Primarily, the policy includes the following to ensure that banks are not used to violate the law.

1. Protrecting Banks from legalizing black money.
2. Adherence to 'Know Your Customer' policy as agreed by the International Group in day-to-day operations.

3. Taking appropriate action when suspicious transactions are noticed and reporing these transactions to the authority established by law.

4. Financial Action Task Force's recommendations on Money Laundering should be followed by International and financial companies and banks as per the agreed norms.

5. Apart from the rules suggested by the RBI, the RE itself may also make further rules regarding ML/TF. **(Amended 10/11/2023 BOD)**

4. **What is Money Laundering ? -**

Money Laundering is not only the laundering of money obtained from illegal transactions, but also the concealment of the chain of many such transactions and concealing the source of money obtained from illegal transactions, including drug trafficking, terrorism, organized crime, fraud and other similar crimes, operations. Simply put, Money Laundering is a process by which the identity and ownership of illegally obtained money is disguised and changed, so that such black money appears to be legitimately obtained.

4 A. Money Laundering and Terrorist Financing Risk Assessment by REs:

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

(b) The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the RE to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies. 345B. REs shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. REs shall implement a CDD programme, having regard to the ML/TF risks identified and the size 16 of business. Further, REs shall monitor the implementation of the controls and enhance them if necessary **(Amended 10/11/2023 BOD)**

5. **Proceeds of Crime-**

Generally, money derived from the following types of serious crime or other similar type of crime:

1. Trafficking / participation in Narcotics.
2. Murder / Attempted Murder.
3. Extortion / Kidnapping for Money.
4. Robberies / Big theft.
5. Frauds / Dealing in fake currency.
6. Offence of dealing in illegal arms.
7. Using / purchasing illegal weapons for legitimate transactions.
8. Crimes relating to wildlife and money derived from that.
9. Money earned from unethical business.
10. Money earned through bribery.
11. Money earned from other criminal and anti-social crimes.

I) **Customer Acceptance Policy-**

1) **Customer Acceptance Policy-**

1. Customers should be classified into three categories by identifying the transaction risk of each customer.

2. Don't open benami / fake / anonymous accounts.

3. Common people who are socially and economically weaker should not be unnecessarily harassed in opening accounts.

4. If the customer does not cooperate in verifying his identity or the documents submitted are not reliable then the account of the concerned customer should not be opened.

5. Account should not be opened without proper information of the customer.

6. The right to request/ask for advance KYC documents/information at any time after account opening should be mentioned at the time of account opening itself.

7. ~~Due diligence of both customers is necessary while opening joint account. (CDD) is very necessary.~~ Bank shall apply the CDD procedure at the UCIC level. Thus if an existing KYC compliant customer of a Bank desires to open another account or avail any other product or service from the Bank, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned. **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

8. The circumstances under which the customer may transact on behalf of others should be clearly stated.

9. CDD should be done at UCIC Level. Because of this, account holders who have KYC clearance will not have to complete KYC again while opening another account.

10. Arrangements should be made to ensure that the deposit does not match the name in the list contained in Chapter ix of the Reserve Bank's Master Direction.

11. Where the PAN is available, the PAN should be checked from the portal of the Issuing Authority.

12. If an E-Document is available from a customer, its verification should be done as per the provisions of the IT Act 2000.

13. Customer's whose GST Details are available, GST Number should be checked from the the portal of Issuing Authority.

14. Where RE forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

15. While opening the account of PEP, the branches must take the written permission of the Senior Officers / Managers.

16. (Section 10) RE shall not open the account of a customer if he does not provide proper CDD while opening the account or the bank is not satisfied that the CDD is genuine or if he is not cooperating. Also RE should do STR if need of such person. **(Amended 10/11/2023 BOD)**

2. **Risk wise classification of Deposit and Loan accounts -**

Some individuals, groups of individuals, firms and companies have created black money by evading various taxes using the banking system in our country. Also, financial scams and chaos have been done using the banking system. Various such professionals have transacted large sums of money. Such transactions are not recorded in their income tax returns. The money obtained from such illegal activities is similar to the money obtained

from foreign countries or from illegal business being used to commit acts harmful to the country. Such incidents have come to the notice of the Government of India. Reserve Bank of India, the central bank of our country has issued Circular No. UBD No DS PVB Cir. 17/13.01.00/2002-03 dated 18.09.2002 Know Your Customer Norms which have been notified to all the banks. According to this circular, every bank has given detailed guidance regarding the care to be taken while opening a new account and the type of documents to be taken from the account holder. After that, following the recommendations made by the Financial Action Task Force regarding Anti Money Laundering Standards and Combating Financing of Terrorism, Reserve Bank has amended the circular dated 18/09/2002 and issued a new circular. Its reference number is UBD.PCB. Cir. 30/09.161.00.2004-05 dated 15/12/2004. Keeping in mind the instructions given in this circular and for implementing this circular a separate policy has been prepared and such policy has been approved in the meeting of the Board of Directors dated 10/02/2005 as per Resolution No. 12. As per the Reserve Bank Circular dated 15.12.2004, all accounts held by the bank branches of the account holder in the form of deposits and loans are required to be classified according to risk. However, the said policy has been prepared regarding how each branch should classify the account holder's accounts. OBJECTIVE - The objective of framing the present policy is to strictly implement the instructions given by the Reserve Bank in the context of Know Your Customer. At present, the following documents are taken from the account holder while opening a new savings and current account.

a) Account opening form in the specimen prepared by the bank is signed by the account holder. The account holder fills all the information in such account opening form. Along with such form, the following information is also taken. It is called Customer Profile. Generally such Customer Profile is taken from Individual. It is used to control transactions on that person's accounts.

1. Occupation / business of the account holder

2. Income sources of the account holder e.g. Salary, business profit, rental income, agricultural income etc.
3. Monthly income of the account holder
4. Annual turnover if business
5. Date of Birth
6. Educational Qualification
7. Details of current loans taken
8. Estimated value of the property in the name of account holder
9. Networth

In case of saving account, it is necessary to get the above information from every new and old account holder. In case of joint account, the details of both the persons are required to be taken as above.

b) Specimen Signature Card

c) A recent photograph of the person who is going to transact the account should be taken.

d) Attested xerox copy of one of the following documents is required to be taken to prove the identity of the account holder.

1. Passport
2. Voter ID Card
3. PAN Card
4. Govt Employment ID card
5. Driving License.
6. Aadhaar Card

All these documents have the photo of the account holder, so his identity is proved. If the account holder has not having PAN number and he is a farmer, then a declaration in Form No. 60 should be taken from him.

Aadhaar card will be considered as ID and Address Proof under KYC policy while proceeding as mentioned above. If Hard Copy of Aadhaar Card is not available then Bank can download E-Aadhaar Card from official site and use it as ID Proof and Address Proof.

e) One of the following documents must be obtained to prove the current residence of the account holder.

1. Electricity Bill
2. Telephone bill
3. Postpaid mobile phone bill
4. Piped gas bill
5. Water bill
6. Salary Slip
7. Income Tax Assessment Order
8. Electricity Bill
9. Ration Card
10. Aadhaar Card

Bank shall not insist on KYC documents of either permanent residential address or current residential address while proceeding as mentioned above under the KYC policy. That is, if the customer submits the KYC documents regarding the permanent resident address, there is no problem in opening the account. Banks should not deter potential customers by insisting on submission of proof of current residential address.

Also, if there is any change in the address submitted by the customer as proof of residence for opening the account, the related documents must be submitted to the bank within three months. If proof of permanent resident address is submitted, proof of the correspondence address need not be taken for doing correspondence. If there is a change in the address of the customer for any reason, the customer is obliged to give an informative notice of the change of address to the bank within two weeks.

f) In case of Current Account following documents are required to be obtained.

1. Copy of the company constitution and regulations as well as company registration certificate, resolution regarding opening of current account in company board of directors meeting, resolution giving authority to use current account, list of directors with name and address.

2. While opening a new current account of the partnership firm, partnership agreement, letter of partnership, certificate of partnership registration (if such certificate is not available, xerox copy of the form and xerox copy of the letter sent for partnership registration and receipt of fee payment)

3. While opening a current account in the name of an educational institution or any registered trust, constitution of that institution, rules/trust deed, certificate of registration, list of board of trustees with address as well as resolution regarding who is authorized to operate the current account.

4. Declaration signed by the applicant while opening a current or saving account in the name of Hindu United Family System (H.U.F.). A letter in a specific format signed by all members of the HUF, photograph of Karta, Karta's residence proof, PAN card or declaration in Form No. 60 etc. Documents should be taken.

5. Important documents as mentioned in 1 to 4 above must be taken according to account holder's organization. Apart from that the following documents should be taken.

1. PAN Card Xerox
2. Statement in Specimen No. 60 if no PAN number
3. The account opening form should bear the signatures of all the partners / account managing trustee and company director. Also photograph, PAN number, proof of residence etc. of all those who are going to operate the account of partnership / trustee / company director documents should be taken.
4. Power Bill / Electricity Bill / Udyog Aadhaar / Business Continuity Certificate etc. in the name of the organization 1 to 3 above. One of the documents should be taken to confirm the business address.
5. The signature of the current account holder in the same branch as the witness or identity should be taken on the account opening form.

Know Your Customer guidelines aim to open a savings or current account only after completing the above documents while opening a new account. In this way every account which has been opened till date through the branches of the bank after completing Know Your Customer needs to be classified according to risk. The details of how to make such a classification are given in the next ~~paragraph~~. **Section (Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

II) Risk Management-

1. Different Risks in Business and actions agaianst them -

1. Reputation Risk -
Credit and reputation of depositors, borrowers and other financial institutions can be jeopardized by such transactions.

2. Compliance Risk -
Punishment / penalty etc. to be imposed on the bank for non-compliance with the guidelines of the relevant Act.

3. Operational Risk -

Compliance with the instructions laid down in this regard / Mistakes made due to incomplete information / Internal errors and business risks arising from external events.

4. Legal Risk -

Risk of legal action against the bank due to non-compliance with legal / guidelines.

5. A comprehensive approach should be taken regarding risk classification of customers.

6. Classification of customer's risk according to a specific reason will be made confidential and no information about it will be given to the customer.

2. According to the Money Laundering Act and its provisions, the bank's relationship with the account holder generally depends on the following.

1. Type of account holder and type of business.
2. Type of product and service availed by the account holder.
3. Name of country of residence. (Geographical position)

3. According to all the above types of classification the account holders will be classified in three ways.

A. High Risk
B. Medium Risk
C. Low Risk

While classifying the risk, the bank should determine the risk of the account holder on the basis of identity, socio-economic status, nature of business, net worth and information about the party's business and its location (Geographic Area).

A) **High Risk** – Business related to the business where Money Laundering is possible

1. Trade in antiquities (individuals and institutions), money service institutions (not employees of institutions) and persons in the arms trade.

2. Each bank should prepare its own list of persons (not citizens) residing in high risk countries and update/revise the same from time to time.

3. Political Foreign Refugees – In such cases banks should get more information about the original source of his money. Such accounts should be opened by a senior officer.

B) **Medium Risk** - All Current Accounts (this will include Listed Companies, Regulated Companies etc.) with a turnover exceeding the Credit Limits required by the Bank for each business.

C) **Low Risk** - All others who are not in either of the above categories will be low risk account holders. Similarly, according to their information, the bank should determine the risk of the account holders and classify them accordingly. All borrowers / customers about whom all information is ascertained can come under this classification.

KYC documents are to be re-verified once in every 2 years for high risk account holders, once in 8 years for medium risk account holders and once in 10 years for low risk account holders while proceeding as mentioned above. If the account holder does not complete the KYC documents along with the PAN card, he should be asked to complete it in next 3 months. If there is no compliance even after that, Debit Freeze the account. But after that the bank can close their account at any time. Also the customer can close the account anytime.

4. Special care should be taken while opening the following types of accounts.

1. Trusts Accounts
2. Account holders without direct interaction while opening the account.
3. Correspondent Banking
4. Fiduciary Account
5. Pooled Accounts

5. Risk Management -

1. As the Bank is required to implement the provisions of AML, the necessary framework, arrangements, controls and other things will be managed.

2. Bank's internal accounting management shall independently assess the necessary legal regulatory requirements regarding the implementation of KYC / AML. Concurrent and internal auditors will check compliance of KYC / AML norms in all branches and report any lapses accordingly. Action Taken Report (ATR) in this regard will be placed before the Audit Committee of the Bank from time to time.

3. All employees will be trained on KYC / AML regulations.

4. The Principal Officer appointed by the bank shall be responsible for all the legal enforcement in this regard.

6. **Customer Training -** Banks need to make customers aware of the legal provisions of KYC/AML and its compliance in bank transactions.

7. Use / Introduction of new Techonologies - Bank will need to regularly adopt new technologies in their opeartions as required for implemenatation of KYC / AML Regulations.

8. KYC verification of existing customers -

1. KYC / AML norms will be applicable to all the existing and new account holders / customers of the bank.

2. All existing accounts will continue to be monitored for KYC / AML.

3. In relation to the existing accounts i.e. companies, shops, households, trusts, charitable organizations, financial organizations and other organizations, it will be necessary to follow the necessary KYC regulations and reporting of suspicious transactions as per the requirements of the law.

9. The Bank shall appoint a Principal Officer who shall be responsible for implementation and completion of KYC/AML. Generally, their duties will include the following:

1. Implementation of KYC/AML norms.
2. To give information about the transaction mentioned therein to the Authority required by law.
3. To liaise with all law enforcement agencies in this regard.
4. Time to time to give necessary information to the top management or board of directors.
5. The Principal Officer should be of RE management level who will provide the information as per MD's rules. **(Amended 10/11/2023 BOD)**

III) Custmor Identification Procedure - (C.I.P.)

1. Key / Highlights of this Policy-

1. Customer Identification -
2. A) First of all complete identification of the account holder / customer.

B) Thereafter to collect all necessary information of that customer, whereby there will be information about the business and related transactions of that customer. This information will be useful to make a profile about him / her.

Bank shall undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.

(b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

(c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(g) Bank shall ensure that introduction is not to be sought while opening accounts.

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

(a) ~~Records or 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.~~

Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry. **(Amended 10/11/2023 BOD)**

(b) Adequate steps are taken by Bank to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.

2. Identification -

1. Verification of account holder's name.
2. Beneficiaries.
3. Signatures of Account Openers.
4. Intermediaries.
5. Customers should be identified as follows.

i. At the time of establishing a business relationship with the bank.
ii. To request additional information from the customer if deemed necessary by looking at the pattern / conduct of transactions in the current customer's account.

iii. Wherever necessary, information about nature of business, location, mode of exchange of funds, total turnover, social and economic status etc., should be taken from the customer for information / identification.

iv. Similarly, customers should be classified into three groups as high risk, medium risk and low risk and it should be reviewed from time to time.

v. It is necessary to identify both the customer who has an account and the customer who does not have an account who has come to transact a large amount once. Similarly, all customers whose financial dealings are likely to pose a threat to the bank's reputation should undergo due diligence.

vi. In order to provide the facility of banking transactions to the general public and not to deprive the people of low income group of this facility, flexibility should be kept in the issue of identity / address documents in case of customers in urban / semi-urban areas. (As per policy of Reserve Bank of India in this regard)

vii. In implementing the Know Your Customer policy, no one will be deprived of banking facilities, especially those who are economically and socially backward. People belonging to low income groups in urban/rural segments should not be denied banking facilities just because they cannot produce identity or residence documents. For those whose balance will not exceed Rs.50,000/-, the simplified Know Your Customer guidelines should be followed. (As per Reserve Bank of India Guidelines)

viii. In exceptional circumstances like death claims, relief etc. For this, the account can be opened by relaxing the KYC rules as above for a person coming once to deposit only the amount of assistance received from the government or other similar institutions.

- **Customer Due Diligence Procedure-**

i. **Customer Due Diligence (CDD) Procedure in case of Individuals**

For undertaking 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, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

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

(ii) he decides to submit his Aadhaar number voluntarily to a bank or any REs notified under first proviso to sub-section (1) of section 11A of the PML Act; or

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

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

(ac) the KYC identifier with an exolicit consent to dounload records from CKYCR

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

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank or to a bank notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or 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 16 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 as specified under Annex I.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC as specified under Annex I.

v) KYC Identifier under clause (ac) above the RE shall retrieve the KYC records online from the CKYCR in accordance with Section 56

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

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, 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 as mandated in Section 8. 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. Explanation 1: bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

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

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made there under.

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

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

ii) [44]As a risk-mitigating measure for such accounts, REs shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. REs shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

iii. the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

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

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

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out, If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

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

viii. 21A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other bank. Further, while uploading KYC information to CKYCR, bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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

Bank may undertake live V-CIP carry out

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 and Section 29, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

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

(a) V-CIP Infrastructure

(i) 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. [50]Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE only and all the data including video recording is transferred to the RE's exclusively

owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

(ii) 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.

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

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

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

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

(vii) [51]The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / 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.

(b) V-CIP Procedure

(i) Each RE 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.

(ii) [51]Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated.

(iii) 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.

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

(v) 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.

(vi) The authorised official of the bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer

d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker

Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

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

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

(vii) 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.

(viii) 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.

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

(x) 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.

(xi) Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks 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.

(xii) 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.

(xiii) All matters not specified under the ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the bank.

V-CIP Records and Data Management

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

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

SMALL Account-

Notwithstanding anything contained in Section 16 (as per MD.-KYC Direction,2016) 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.

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 between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.

(h) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per Section 16 or Section 18.

(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 16 or Section 18.

Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs): In case a person who desires to open an account is not able to produce

documents, as specified in Section 16, NBFCs may at their discretion open accounts subject to the following conditions:

(a) The NBFC shall obtain a self-attested photograph from the customer.

(b) The designated officer of the NBFC certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) 65The account shall remain operational initially for a period of twelve months, within which CDD as per Section 16 or Section 18 shall be carried out.

(d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time. 29

(e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

(g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

(h) "The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per Section 16 or Section 18." **(Amended 10/11/2023 BOD)**

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

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-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government

(b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

(c) Sales and income tax returns.

(d) [71]CST/VAT/ GST certificate.

(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 or Licence/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, landline telephone bills, etc.

In cases where it is not possible to furnish two such documents, bank may, accept only one of those documents as proof of business/activity.

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

CDD Measures for Legal Entities

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

(a) Certificate of incorporation

(b) Memorandum and Articles of Association

(c) Permanent Account Number of the company

(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

(e) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

(f) [75]the names of the relevant persons holding senior management position; and

(g) [76]the registered office and the principal place of its business, if it is different.

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

(a) Registration certificate

(b) Partnership deed

(c) Permanent Account Number of the partnership firm

(d) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

(e) [80]the names of all the partners and

(f) [81]address of the registered office, and the principal place of its business, if it is different.

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

(a) Registration certificate

(b) Trust deed

(c) Permanent Account Number or Form No.60 of the trust

(d) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

(e) [85]the names of the beneficiaries, trustees, settlor, protector if any and authors of the trust **(Amended 10/11/2023 BOD)**

(f) [86]the address of the registered office of the trust; and

(g) [87]list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

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-documents thereof shall be obtained:

(a) Resolution of the managing body of such association or body of individuals

(b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals

(c) Power of attorney granted to transact on its behalf

(d) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and

(e) 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.

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

(a) Document showing name of the person authorised to act on behalf of the entity;

(b) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and

(c) Such documents as may be required by the bank to establish the legal existence of such an entity/juridical person.

Provided that in case of a trust, the RE shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of Section 13 of this MD.

(Amended 10/11/2023 BOD)

Identification of Beneficial Owner

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

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

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

On-going Due Diligence

RE 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 / wealth. **(Amended 10/11/2023 BOD)**

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.

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

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 Multi-level 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.~~ Explanation has been shifted **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

II. Updation / 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. Policy in this regard shall be documented as part of REs' internal KYC policy duly~~

~~approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.~~

REs shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. 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. Policy in this regard shall be documented as part of REs' internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated. **(Amended 10/11/2023 BOD)**

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

ii. Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the RE, customer's mobile number registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), 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.

~~Further, REs, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for 33 the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the REs in their internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.~~

Further, REs, at their option, may obtain a copy of OVD or deemed OVD, as defined in Section 3(a)(xiv), or the equivalent e-documents thereof, as defined in Section 3(a)(x), for the purpose of proof of address, declared by the customer at the time of **periodic updation (Amended as per**

DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024). Such requirement, however, shall be clearly specified by the REs in their internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated. (Amended 10/11/2023 BOD)

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

iv. 94Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** To clarify, conditions stipulated in Section 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. REs shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals: i. No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), letter from an official authorized by the LE in this regard, board resolution, etc. Further, REs shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

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

c) [95]Additional measures: In addition to the above, REs shall ensure that,

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

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

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**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 REs and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, REs may consider making available the facility of periodic updation **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.

v. REs shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the REs such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the RE where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.

d) [96]REs shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment

of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the REs the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at REs' end.

In case of existing customers, bank shall obtain the Permanent Account Number or 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 equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the RE shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, RE shall give relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or 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. Such accounts shall, however, be subject to enhanced monitoring.

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

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

Updation/periodic updation of KYC - Simplified procedures :

(a) Bank will do risk categorization of individuals is done through a proper process of due diligence based on ML/TF nsk assessment in the account-based relationship rather than bulk-categorization of accounts based on a single or a very broad parameter.

(b) Bank will ensure that an individual customer has a Unique Customer Identification Code

(UCIC) and KYC updation is done at UCIC level rather than at the account level. This will eliminate the need for customer to undergo multiple KYC updation.

(d)Banks infrastructure and systems are put in place to receive/process self-declaration from customers in cases where there is no change in KYC information, through options such as registered mobile number/ email-id, ATMs, internet/mobile banking, etc. Availability of these options should also be communicated to customers while asking for KYC updation.

(e) Submission of physical copy of such self-declarations or any other KYC documents for updation of information will be enable at any branch of the bank without insisting the customer to visit the 'home' branch.

(f) Communication from customers for change in address should be received through either of channels mentioned at sub-paragraphs (d)i.e. registered mobile number/ email-id, ATMs, internet/mobile banking, etc. & (e)i.e. KYC documents for updation of information will be enable at any branch of the bank, above to follow the process prescribed at section 38(a)(ii) ibid.

(g) Front-end staff will be sensitize about the benefits of CKYCR and various simplifications carried out in the KYC process and non-insistence on Aadhaar number/card for KYC purpose.

(h) Customer's visit to branch or any interaction with the customer for other purposes be leveraged for KYC updation where periodic KYC updation may be impending or pending, and accordingly, reset the next due date.

(i) Bank will create awareness among the relevant staff regarding the simplified procedures for updation/ periodic updation of KYC and communicating same to the customers. This, in fact, may reduce the need for branch visits or additional communication with customers for updation of KYC.

(ii) Wherever possible bank will guide customers by the branches to ascertain the available modes/options for updating KYC details as a means to caution them against frauds in the name of KYC updation. In this context, a reference may be made to the Press Release dated February 2, 2024, wherein bank had cautioned the public in this regard. **(AMENDED 23/08/2024 BOD – RBI Circular Dated 25/07/2024 DOR.AML.No.2158/14 .01.001/2024-25)**

Enhanced and Simplified Due Diligence Procedure

Enhanced Due Diligence

[98]Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17): Non-face-to-face onboarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by REs for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

a) In case RE has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. RE shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, RE shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) RE shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer. 37

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP

Accounts of Politically Exposed Persons (PEPs) –

~~A. Bank shall have the option of establishing a relationship with PEPs provided that:~~

~~(a) Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;~~ **(AMENDED 10/11/2023 BOD)**

"Explanation: For the purpose of this Section, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials."**(Amended MD CIR 04/01/2024 BOD 12/01/2024)**

~~(b) The identity of the person shall have been verified before accepting the PEP as a customer;~~

~~(c) The decision to open an account for a PEP is taken at a senior level in accordance with the bank Customer Acceptance Policy;~~

~~(d) All such accounts are subjected to enhance monitoring on an on-going basis;~~

~~(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;~~

~~(f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.~~

~~B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner~~ **(AMENDED 10/11/2023 BOD)**

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

(a) REs have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

(b) Reasonable measures are taken by the REs for establishing the source of funds / wealth;

(c) the approval to open an account for a PEP shall be obtained from the senior management;

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

B. These instructions shall also be applicable to family members or close associates of PEPs. **(Amended 10/11/2023 BOD)**

Client accounts opened by professional intermediaries:

Bank shall ensure while opening client accounts through professional intermediaries, that:

(a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

(b)Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

(c) Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the bank.

(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of bank, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of bank, the bank shall look for the beneficial owners.

(e) Bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

(f) The ultimate responsibility for knowing the customer lies with the bank.

B. Simplified Due Diligence

Simplified norms for Self Help Groups (SHGs)

(a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.

(b) CDD of all the office bearers shall suffice.

(c) No separate CDD as per the CDD procedure mentioned in Section 16 of the MD of the members or office bearers shall be necessary at the time of credit linking of SHGs.

Procedure to be followed by banks while opening accounts of foreign students

(a) Banks shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

(b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.

(c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. RE shall, **(Amended 10/11/2023 BOD)**

(a) Maintain all necessary records of transactions between the bank and the customer, both domestic and international, for at least five years from the date of transaction;

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

(c) Make available swiftly, the identification records and transaction data to the competent authorities upon request;

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

(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) The nature of the transactions;

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

(iii) The date on which the transaction was conducted; and

(iv) The parties to the transaction.

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

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

. [102]Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

DARPAN PORTAL REGISTRATION

REs shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, RE shall register the details on the DARPAN Portal. REs shall also maintain such registration records for a period of five years after the business relationship between the customer and the RE has ended or the account has been closed, whichever is later. **(Amended 10/11/2023 BOD)**

Reporting Requirements to Financial Intelligence Unit - India

REs shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those REs, whose all branches are not fully computerized, shall have suitable arrangement to cull

out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. REs shall not put any restriction on operations in the accounts where an STR has been filed. ~~REs shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.~~

~~Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions. Chapter IX~~

Every RE, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done. **(Amended 10/11/2023 BOD)**

Requirements/obligations under International Agreements - Communications from International Agencies

[103]Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(a) REs shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and 42 periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

i. The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and

entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

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

(b) Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated 104February 2, 2021 (Annex II of this Master Direction).

(c) Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 105February 2, 2021 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of ~~Nodal Officers~~ for UAPA is available on the website of MHA.

'Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967', the designation of Central Nodal Officer for the UAPA has been changed from "Additional Secretary" to "Joint Secretary". **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

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

(a) REs shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) 43 and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the

WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

(b) In accordance with ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** 3 of the aforementioned Order, REs shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

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

(d) In case of match in the above cases, REs shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the ~~Central Nodal Officer (CNO),~~ designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. ~~REs shall file an STR with FIU - IND covering all transactions in the accounts, covered above, carried through or attempted.~~ It may be noted that in terms of ~~Paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** 1 of the Order, Director, FIU-India has been designated as the CNO.

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

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

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

(h) The process of unfreezing of funds, etc., shall be observed as per ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be

forwarded by RE along with full 44 details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

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

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

Countermeasures

REs shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government. **(Amended 10/11/2023 BOD)**

Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. ~~Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.~~ REs shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. **(Amended 10/11/2023 BOD)**

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

FATF Statements. Explanation: The processes referred to in (a) & (b) above do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

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

[108]REs are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

Other instructions

Secrecy Obligations and Sharing of Information:

(a) REs shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the RE and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, REs shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of RE requires disclosure and

iv. Where the disclosure is made with the express or implied consent of the customer.

Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010 (Not Applicable to us) (Amended 10/11/2023 BOD)

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

(a) 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.

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

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(d) 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.

(e) Bank has required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

(f) 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.

(g) Once KYC Identifier is generated by CKYCR, bank shall ensure that the same is communicated to the individual/LE as the case may be.

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as

specified in ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer. Also whenever the bank obtains additional or updated information from any customer as per clause (j) below in this ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** or Rule 9(1C) of the PML Rules, the RE shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an bank regarding an update in the KYC record of an existing customer, the bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the bank. **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

(i) Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(j) ~~Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to a bank, with an explicit consent to download records from CKYCR, then such 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.~~

~~iv) [111]the validity period of documents downloaded from CKYCR has lapsed.~~

(j) For the purpose of establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, the bank shall seek the KYC

Identifier from the customer or retrieve the KYC identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless –

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

(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or

(iii) the validity period of downloaded documents has lapsed; or

(iv) the bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer. **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)**

Period for presenting payment instruments

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

Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules."

Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the concerned bank, it shall then be deemed that the bank has not complied with these directions. **(Amended 10/11/2023 BOD)**

Instructions received from RBI in Advisory regarding Use of money mule accounts for cyber – enabled frauds. (Ref.No.CO.DOS.RSB.No.S6058/11-01-006/2024-2025) dated November 19, 2024.

1. ensure strict adherence to customer due diligence requirements during opening of accounts and monitoring of newly opened accounts, in order to restrict mule accounts and their operations.
2. ensure that alerts are generated and examined in case of abnormally frequent and large transactions in domestic bank accounts being carried out from locations including from overseas jurisdictions, not matching with the usual location / economic / financial profile of the customer.
3. carry out comprehensive analysis of the accounts being used / identified as suspected money mule accounts and strengthen the risk monitoring rules based on the same.
4. review various customer onboarding processes adopted by the bank and address gaps / vulnerabilities being exploited by the fraudsters, particularly in accounts opened trough non – face – to face mode, V-CIP, Aadhaar OTP based e-KYC accounts, accounts opened from particular areas / locations where frauds / cyber – crimes are more prevalent (hotspots) etc.
5. put in place an IP based transaction monitoring system and identify unusual pattern of transactions both for domestic and from overseas jurisdictions. Further, in view of the recent inputs on cybercrimes being perpetrated from locations in South-East Asia, particularly from Cambodia, Myanmar and Laos PDR, special attention may be provided to Indian bank accounts being operated from such jurisdictions. The necessary inputs in this regard may also be obtained from I4C,MHA, GoI on a regular basis. The banks may also put in place restriction on usage of transaction from overseas IPs, based on the customer profile.
6. monitor cash withdrawals made trough overseas ATMs and at ATMs outside the State where the customer resides or at locations which are hotspots and examine the need for transaction restrictions on use of Indian Debit Cards abroad, especially from Dubai, Kazakhstan and Thailand.

7. monitor cash withdrawals through cheques made from domestic branches of banks especially in hotspot regions. Necessary inputs in this regard may be obtained from I4C,MHA.
8. monitor loading of prepaid wallets issued by foreign entities, using domestic debit / credit cards / bank accounts.
9. ensure deployment and adoption of robust software for real – time transaction monitoring and use of AI / ML tools in detecting suspicious and fraudulent transaction patterns as well as use of network analytics in identifying mule networks. Setting up of a dedicated centralised unit at the bank – level may also be considered for a harmonised and time bound response in countering cyber – enabled frauds.
10. fix a shorter Turn-Around-Time (TAT) for processing alerts pertaining to money mules / cyber – enabled frauds and for reporting STRs, as may be required.
11. have robust mechanism for change of mobile number by customers, and also monitor such customers who frequently change their mobile numbers, through Enhanced Due Diligence.
12. carry out Enhanced Due Diligence of current accounts wherein there are huge volume of transactions, inconsistent with the declared turnover and business profile, as in many cases, it has been observed that current accounts opened by Sole Proprietorship firms using Udyam Registration Certificate (MSME) are used to transfer / layer the proceeds of crime.
13. subject accounts that are being repeatedly reported to the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) to Enhanced Due Diligence and take action as per PML Act, 2002 and analyse such accounts on the reasons for opening and their repeated usage in channelling fraudulent proceeds. In this regard, any instruction received from Law Enforcement Agencies (LEAs) shall be adhered to as per the extant law.
14. include the typologies on cyber-enabled frauds and use of money mule accounts as part of the training curriculum in the bank, so as to sensitise the staff,

particularly those who are required to deal with KYC / AML matters an Transaction Monitoring.

(Amended 13/12/2024 BOD)

Collection of Account Payee Cheques

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.

(a) [112]A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by REs.

(b) [113]The REs shall, at their option, not issue UCIC to all walk-in/occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

[114]Introduction of New Technologies

REs shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery 49 mechanisms, and the use of new or developing technologies for both new and pre-existing products. Further, REs shall ensure: (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

[115]Correspondent Banking

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent

banking and other similar relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

~~(a) Sufficient information in relation to the nature of business of the respondent including information on management, major business activities, level of AML/CFT controls, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country, and publicly available information regarding the reputation of the institution and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action, shall be gathered.~~

~~(b) Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.~~

~~(c) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented and understood~~.

(a) Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.

(b) The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.

(c) Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.

(d) Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved. **(Amended 10/11/2023 BOD)**

(e) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.

(f) The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.

(g) Correspondent relationship shall not be entered into with a shell bank.

(h)It shall be ensured that the correspondent banks do not permit their accounts to be used by shell banks.

(i)Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

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

Wire transfer (Not Applicable to us) (Amended 10/11/2023 BOD)

Issue and Payment of Demand Drafts, etc.,

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

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

Quoting of PAN

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

Selling Third party products

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

(a) The identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

(b) Transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

(c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) Transactions involving rupees fifty thousand and above shall be undertaken only by:

-Debit to customers' account or against cheques; and
- obtaining and verifying the PAN given by the account-based as well as walk-in customers.

(e) Instruction at 'd' above shall also apply to sale of bank own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

At-par cheque facility availed by bank

(a) Banks shall:

i. ensure that the 'at par' cheque facility is utilised only:

a. for their own use,

b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,

c. for walk-in customers against cash for less than rupees fifty thousand per individual.

ii. Maintain the following:

a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,

b. sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

iii. Ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

Issuance of Prepaid Payment Instruments (PPIs):

PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

[117]Hiring of Employees and Employee training

(a) Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) REs shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall 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 RE, regulation and related issues shall be ensured

Digital KYC Process

A.The bank shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the bank.

B. The access of the Application shall be controlled by the bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by bank to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the bank or vice-versa. The original OVD shall be in possession of the customer.

D. The bank must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the bank shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. the Application of the bank shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead

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

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

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

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

L. The authorized officer of the bank shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

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

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

III) Basic Principals & Objectives of Money Laundeing Prevention & Compliance

All banks should adopt the following principles while complying with the laws and regulations passed by the Indian Legislature.

1. Policies, regulations and controls should be designed to prevent criminals from laundering the proceeds of crime.

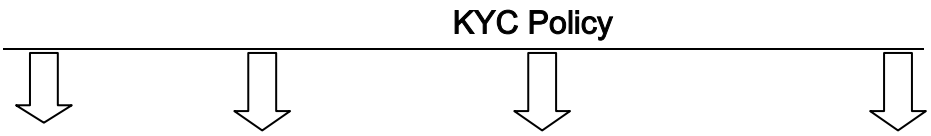
2. Banks should be aware of the risks involved in designing the rules and controls for such policy matters. Banks should strictly implement their policies and regulations by understanding the risks involved in them. So that the policies and regulations will not fall below the standards of the guidelines.

3. Implementation of 'Know Your Customer' policies should be done satisfactorily in such a way that the main beneficiary availing the banking service and the source of incoming money-deposit, remittance, investment etc. as informed by the account holder should be satisfactorily verified. In this, the nature and information about the business generally done by the account holder and the irregular transactions arising from it will be carefully kept.

4. A person with proper seniority, integrity and independence should be appointed as "Principal Officer", who will follow all the procedures related to Money Laundering and submit regular information about it to the Board of Directors.

5. It will be necessary to appoint him as a central person to implement the law in this regard as well as to maintain contact with the department. In this regard, he can take help of Fraud Control / Vigilance etc. Departments.

6. It is essential that bank have a **KYC Policy,** which is approved by the Board of Directors.



Customer Acceptance **Risk Management** **Customer Identificaction Procedure (CIP)** **Monitoring of Transactions Policy**

1) **Designated Director-**

The Board of Directors has to appoint a **Designated Director**. And the name, address, email and position of the concerned director is to be reported to **FIU-IND**. It is also necessary to report to **RBI**. Where there is no **Designated Director**, **Principal Officer** should be appointed as **Designated Director**.

2) **Principal Officer-**

The **Principal Officer** appointed on behalf of the Bank is to ensure that all necessary information/reports regarding **KYC / AML** are filed in time. He is responsible for ensuring **Monitoring Transaction, Sharing & Reporting**. The Principal Officer should be a senior officer in the Bank. The appointed principal officer has to preserve the **records** and information regarding **Anti-Money Laundering** for at least 5 years. He should provide information promptly if requested for inspection by **RBI Inspector / Auditor**. Division of responsibilities for efficient implementation of KYC policy. Legal and regulatory review of policies.

Such reports will be prepared and sent from the live transaction data of the bank in the pattern and period decided by FIU-India.

3) Compliance of KYC Policy- Compliance and monitoring of KYC Policy -

a) Determining the responsibility of senior management regarding KYC.

b) Fixing responsibility at different levels.

c) Taking opinion from internal / con-current auditors regarding KYC Policy and action accordingly.

d) Also submitting a note regarding KYC completion to the Audit Committee every quarter.

4. All unexplained, irregular and suspected criminal transactions should be reported to the **Principal Officer**, after which the **Principal Officer** will investigate the transaction and send a **report** to the appropriate authority.

5. **Reports** of suspicious transactions should be unambiguous and should be sent to the **Principal Officer** without any delay.

6. All employees should have the right to know the source of the information to realize their statutory responsibilities and bank should inform the concerned employees about the **Antimoney Laundering** policy adopted by the bank. Appropriate training on **Antimoney Laundering** should be imparted to the concerned personnel so that they are aware of the dangers involved in doing banking business. A **record** of such trained personnel should be maintained.

7. All documents regarding the account holder's identity should be preserved for five years after the end of the business relationship.

8. Awarness and concern for Rederessal of Defects

"What is Suspicious?"

"Suspicious transaction" as defined in the **PMLA** Act means a transaction (whether in cash or not) which is not made in **good faith**.

1. Where there is suspicion that the money has come through criminal means.
2. Money may appear to have been obtained in more unusual, inappropriate ways than usual.
3. For which there is no good reason.

(This includes withdrawal of deposit, transfer or change in any currency, payment by cash or cheque, order or other document through electronic or non-physical means)

The PML Act has made it the responsibility of banks to report such suspicious transactions within three days. Suspicion is personal and impersonal and falls short of proof in the absence of evidence. If doubt is to be defined as beyond reason, some things are grounds for doubt, a test of satisfaction. That is, not full belief, but at least less factual basis for belief and suspicion beyond the logic of whether an event has occurred, but it must be based on something solid.

9. What is Meant by Reasonable grounds of suspect:-

Willfully or recklessly disregarding something, failing to make the inquiries that a reasonable person would make in the circumstances, or failing to make the inquiries that a reasonable person would make based on the information presented or the facts before them. The staff of the bank should, in a certain situation, extract the correct information of

the account holder in a reliable manner and find the justification for any transaction which seems suspicious.

10."Know Your Customer" - The Basis for reporting Suspicion-

For this, proper training should be given to the relevant staff, so that they know which transaction is suspicious or there is full scope to suspect that Money Laundering Transaction is taking place.

This training will give employees the ability to determine whether the transaction is regular or not. For this, the bank employee can decide whether the account holder and the related transaction is correct or not and can check it properly.

Adequate adherence to the policy of "Know Your Customer" will help detect irregular and suspicious transactions. Knowing the details of the account holder and the movements or instructions of the account holder and the related transactions will be the key point to know the suspicious transactions.

V) Monitoring of Transactions

1. Control over Customer Transactions -

1. Each account and the account holder's risk shall be monitored and controlled.
2. Special attention will be given to large transactions that are complex and out of the ordinary. Such transactions have no financial or viable legal purpose.
3. Transactions involving large amounts of cash that are inconsistent and different from the usual expected behavior of customers will normally be subject to special and thorough scrutiny.

4. Suspicious and similar transactions covered by PML Act 2002 shall be referred to the appropriate legal authority after proper investigation and all such cases, documents shall be preserved for the period mentioned in the Act.

2. In general, the following types of transactions should be deemed to have taken place under suspicious circumstances-

1. There is no compelling reason to do the transaction and no economic reason behind it.
2. The transaction done by the account holder will be different from the regular transaction done by him and will not be compatible.
3. The account holder will be reluctant to provide more information about a particular transaction if inquired about.
4. Doing offshore transactions with other companies which seem unnecessary in terms of business and which have no need for regular transactions of the account holder.
5. Unnecessary remittances from third party accounts.
6. Dealing in investment without any motive of profit.

Apart from the above mentioned such transactions should be reported to **FIU-IND** keeping in view the norms based on the rules laid down in the **Money Laundering Act**.

3. Classification according to Risk

At present, savings and current accounts which have been opened with various banks are deposited with large amounts in cash. Similarly, large amounts of cash are withdrawn from such accounts. Such amounts are appropriated for anti-national terrorist activities. Also, some individuals open accounts in benami names to evade taxes like income tax, wealth tax, service tax, sales tax, excise duty and make large financial transactions from such accounts. This is how the black money is generated. Such generation of black money creates a parallel economy and increases real estate prices tremendously. Similarly, it harms the progress and development of the country. It is necessary to control

the financial transactions by considering all these aspects. Keeping this matter in mind, the central government has taken measures from time to time to prevent the generation of black money and curb illegal transactions. As the Reserve Bank is the central bank that controls all the banks in the country, instructions have been given to all the banks through such a bank to follow the Know Your Customer norms. Also, in order to control the cash transactions in the savings and current accounts with the bank, every bank has instructed to send the information of the transactions in the form of Cash Transaction Report (CTR) to Delhi in the form of Cash Transaction Report, in which the amount of deposits and cash transactions in the form of more than Rs. 5 lakh have been done every month. Also, instructions have been given to all the banks to send Suspicious Transaction Report (STR) of the account on which there are suspicious transactions. Also, instructions have been given to periodically scrutinize all the accounts held by the bank and categorize such accounts into low risk, medium risk, and high risk. At the time of opening a new account, such risk classification is to be done and from time to time, the basic risk classification is to be changed if the low and medium risk accounts go into higher risk category after reviewing such risk. The following ~~paragraph~~ section **(Amended as per DOR.AML.REC.49/1401.001/2024-25 dated-06/11/2024)** provides details on which accounts are classified as low risk, medium risk or high risk.

1. Low Risk Accounts:

The following types of accounts will be included in the low risk category.

- Savings accounts opened by salaried employee class, pensioner class
- Accounts opened by low income group individuals
- Accounts where the sum of Credit / Debit transactions is less than Rs.10 lakhs in a year.
- Small Businessmen and Companies whose total Credit / Debit transactions in a year are less than Rs.10 lakhs.
- Gold loans amounting to Rs. 2 lakhs and less.

- All types of deposit loans (except overdraft loans)
- Fixed Deposits of less than Rs.50,000/- (However, any amount deposited by a Class A member can be included in this account)
- Accounts opened in the name of organizations such as Rotary Club, Giants Club, Lawyers or Doctors or Chartered Accountants
- All types of Pygmy and Recurring Deposit Accounts
- All types of bank guarantees where 100% deposit is taken
- Accounts, which are not classified as high risk and moderate risk

2. Medium Risk Accounts:

The following types of accounts will be classified under this category,

-Savings accounts opened by persons other than salaried, pensioners, low income earners will be classified into this type up to six months from the date of opening of the account. Such accounts will be reclassified after reviewing the transactions on this account in six months
- Current Account of a Proprietary Firm in which a person is engaged in business
-Accounts opened in the name of partnership firm, company, cooperative society, educational institution, private limited company, limited company
-Accounts where the sum of credit / debit side transactions is more than Rs.10 lakh and less than Rs.1 crore in a year.
-Gold Loans amounting to Rs. 2 lakhs and less than Rs.5 lakhs.
-Loan on Deposit, Overdraft Account
- Fixed Deposits from Rs.50,000 to Rs.5,00,000
- All types of bank guarantees where an amount less than the guaranteed amount is taken as deposit
-Accounts, which are not classified as low risk and high risk

3. High Risk Accounts:

The following types of accounts will be classified under this category,

- Current and Savings Accounts in which the sum of transactions in Debit / Credit side in a year is more than Rs. 1.00 crores.

- Accounts of trusts other than educational institutions, accounts of unregistered institutions, temples, clubs, associations

- Accounts in which another person transacts on behalf of the account holder and the account holder does not transact.

- Accounts where the sum of Debit / Credit transactions are more than Rs.1 Crore in a year. (In case of new account, classification should be done by estimating the annual turnover according to the income of the individual)

- Gold Loan accounts amounting to Rs. 5.00 Lakhs and more.

-Savings, Current and Loan account of the account holder whose Cheques are get frequently dishonoured.

- Fixed Deposits of Rs. 5,00,001/- and more

-All types of Bank Guarantees where the guarantee amount is demanded by the Beneficiary. (Devolved Bank Guarantee)

- Accounts classified under NPA loan category

- Savings account of the account holder against whom action has been taken for tax evasion or fraud and current account in the name of the proprietary firm

- Accounts which are not classified as Low Risk and Medium Risk

- Builders & Developers and accounts of Goldsmiths

- All types of accounts of Jewellers

- Wildlife trade related accounts (including domestic animals and pets) as per following classification points –

1) Client Profile Base Classification –

a) Industries like forestry resources, wildlife trade, traditional medicine, and manufacturing of items such as bone carvings or faux fur etc.

b) Entities involved in wildlife-related industries such as private zoos, breeders, pet stores, safari companies, aquariums, and wildlife reserves.

c) Individual/Firm involved in skin and leather goods trading with a high credit turnover and incoming transfers from unrelated parties.

d) Individuals or businesses with adverse media exposure, or identified connections to known wildlife traffickers or organized crime networks

e) A large volume of cash deposits and withdrawals in accounts of state/central government officials who are working in forest department such as forest officers or rangers, may indicate involvement in bribery, corruption, for facilitation of wildlife trafficking.

f) Charitable trusts or societies operating cattle shelters without registration with governing or regulatory bodies like NITI Aayog or the Animal Welfare Board of India.

g) Accounts receiving third-party wire transfers or huge cash deposits, or showing withdrawals by known wildlife poachers and traffickers.

h) Large wire transfers between wildlife farms / firms in unrelated or inconsistent industries.

2) Client Transaction Base Classification –

a) Transaction descriptions or communication details (e.g., email addresses, remittance information, and payment references) that include terms associated with illegal wildlife trade, such as endangered species or animal parts (e.g., ivory, tusks, scales, shark fins, tortoises, or geckos).

b) A large number of small-value UPI (Unified Payments Interface) or IMPS (Immediate Payment Service) credits and deposits linked to the sale of Ayurvedic health products, especially when the amounts are below typical transaction thresholds that would raise suspicion for large-scale purchases.

c) Frequent or unusual card/ATM usage in locations that are either the source or destination points for wildlife trafficking, or in towns and countries historically known for illegal wildlife trade routes.

3) Client Location Base Classification –

a) Geographical proximity of slaughterhouses to designated wildlife zones or sanctuaries, especially when these facilities are located in regions known for illegal wildlife trade.
b) Unusual patterns of activity at recreational businesses (such as resorts, water sports activities, selling of souvenirs and tourism-related services) located within or near wildlife sanctuaries or protected areas, particularly if they are in remote regions with limited law enforcement or oversight. **(Amended 13/12/2024 BOD)**

Note:

1. If one account of an account holder is in high risk category and other accounts are in low risk or medium risk category then all his accounts in the branch should be classified in high risk category.

2. If there is a change in the risk after reviewing the account every quarter, such change will be made at the branch level.

3. The risk-wise classification of the account shall not be communicated to the concerned account holder as well as to other account holders and others. Such classification shall be kept confidential. However, if the respective account holder is going to open an account with other branches of the bank, such category information will be given to the concerned branch.

4. If the Concurrent Auditor of the branch, Internal Auditor, Statutory Auditor as well as Internal Audit from the Head Office suggest about changing the risk category then the risk category should be changed by the Branch after taking approval of the Head Office.

To review the classification made by the branches

Head Office will review every month whether or not all accounts of branches have been classified as risk-wise. For that, a confirmation letter regarding classification will be taken from the branch every month. Also, the data will be requested from the branches in the prescribed format. Based on that, the head office will prepare aggregate statistics

regarding risk. Also, a report regarding suspicious transactions will be requested from the branches in the prescribed format.

5. The **KYC / AML** policy will be reviewed as necessary and placed before the Board of Directors for approval.

****