Know Your Customer (KYC) Guidelines & Anti-Money Laundering (AML) Policy

Document Title	Know Your Customer (KYC) Guidelines & Anti-Money Laundering (AML) Policy
Effective Date	Board Approval Date
Frequency of review	Annual
Document Owner	Compliance department of the Company
Document Approver	Board of Directors

Review:

Version	Last Review Date
Version 1.0	March 27, 2017
Version 2.0	March 28, 2018
Version 3.0	March 18, 2020
Version 4.0	June 29, 2021
Version 5.0	May 24, 2022
Version 6.0	May 26, 2023

Table of Contents

1. Preamble

The Reserve Bank of India (RBI) has issued guidelines on Know Your Customer and Anti-Money Laundering and has advised all the NBFC's to ensure that a policy on KYC and AML measures is formulated and approved by the Board of Fedbank Financial Services Ltd or any another Committee of the Board to which powers has been delegated.

The policy is prepared in line with the RBI guidelines and proposed to be revised with the approval of the Board. The Policy shall be applicable to all the products and services offered by the Company.

2. Know Your Customer Guidelines and Anti-Money Laundering Standards

The objective of the KYC Guidelines is to:

- Adhere to the guidelines issued by RBI in terms of Prevention of Money-Laundering Act 2002, the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 as amended from time to time.
- Adhere to the KYC guidelines issued by RBI Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time.
- To prevent company from being used intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The following four key elements form a part of the policy:

- Customer Acceptance Policy
- Customer Identification Procedures
- Risk Management
- Monitoring of Transactions

3. Definitions

"Beneficial Owner" is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercise ultimate effective control over a judicial person.

"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.

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

"Customer identification" means undertaking the process of CDD.

"Certified Copy" - Obtaining a certified copy by the Company 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.

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.

"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.

"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).

"Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

"Officially Valid Document" (OVD) means

1) the passport,
2) the driving licence,
3) Proof of possession of Aadhaar number,
4) the Voter's Identity Card issued by the Election Commission of India,
5) Job card issued by NREGA duly signed by an officer of the State Government and
6) Letter issued by the National Population Register containing details of name and address.

Provided that,

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

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

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

The customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

c. 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.

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.

"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).

"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.

"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. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

"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.

"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.

"Video-based Customer Identification Process (V-CIP)" is 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 Customer KYC.

"Senior Management" would include personnel of the company who are members of the core management team excluding Board of Directors comprising all members of management one level below the executive directors, including that of functional heads. For the purpose of this policy & in specific to opening of accounts for a PEP "Senior Management" would mean approval from Head of Credit or Risk.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time.

4. Designated Director and Principal Officer

The Managing Director and CEO of the Company shall be appointed as Designated Director by the Board of Fedfina for ensuring obligations imposed under Chapter IV of the PML Act and the Rules as defined from time to time.

The Company shall appoint a Principal Officer, as required under the Prevention of Money Laundering Act, 2002. For the purpose of this policy the Principal officer would mean the officer nominated by the Board of Fedfina, responsible for furnishing information and undertaking such other obligations as required under PMLA Act , rules and any other laws/ regulations as applicable.

5. Customer Acceptance Policy

The Customer Acceptance Policy lays down explicit criteria for acceptance of customers. The Policy ensures that the following procedures shall be followed in relation to customer who approach for availing financial facilities with the Company.

a) No account is opened in anonymous or fictitious names or on behalf of other persons whose identity has not been disclosed or cannot be verified.
b) Parameters of risk perception are clearly defined in terms of nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status.
c) Customers would be categorised as low, medium and high risk.
d) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
e) Not to open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e. company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the company.
f) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there would be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.
g) Necessary checks will be done before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or sanction list etc.
h) The nature and extent of due diligence will depend on the risk perceived by the company. However, while preparing customer profile, branches/offices should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
i) A system is required to be put in place for periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher

risk perception on a customer. Such review of risk categorization of customers should be carried out at regular intervals as prescribed by Risk Department of the company.

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

k) Permanent Account Number (PAN) obtained shall be verified from the verification facility of the issuing authority.

l) Wherever Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority

m) Any additional information not specified herein shall be obtained with the explicit consent of the customer

6. Customer Identification Procedure

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Company need to obtain sufficient information necessary to establish, to their satisfaction, **the identity** of each new customer, whether regular or occasional, and **the purpose** of the intended nature of relationship.

- The first requirement of customer identification procedures to be satisfied is that a prospective customer is the person who he/she claims to be.
- The second requirement of customer identification procedures is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions.
- Customers dentity shall be verified for:-
  - ✓ The named account holder;
  - ✓ Beneficial owners;
  - ✓ Signatories to an account; and
  - ✓ Intermediate parties.
- The Customer Identification Procedures are to be carried out at the following stages:
  - ✓ While establishing a new business relationship;
  - ✓ Periodically as part of KYC review or when the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.
- Copies of the documents produced as Proof of Identity and Address shall be obtained and retained with the Company, wherein a responsible Company Official has to attest such copies certifying that the Originals thereof have been verified.
- The periodicity of updating of customer's identification data should be done once in ten years in case of low risk category customers, once in eight years in case of medium risk category customers and once in two years in case of high risk categories.
- Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.
- Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure-1**.
- Also, the information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes. It will be ensured that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard.

- Any additional information from the customer should be sought separately with his /her consent.

7. Customer Due Diligence (CDD)

1. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose.
   Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.
2. Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Annexure I&II or V-CIP is carried out
3. If Aadhaar details are used for V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
4. The Company may undertake V-CIP to carry out:
   a. 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.
   b. Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Annexure 1, apart from undertaking CDD of the proprietor.
   c. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication shall be subject to conditions laid down in Master Directions, updated from time to time.
   d. Updation/Periodic updation of KYC for eligible customers.
5. While undertaking V-CIP, the Company shall adhere to minimum standards as mentioned in Annexure IV.
6. The decision making functions of determining compliance with KYC norms should not be outsourced.
7. CDD procedure should be applied at the UCIC level and if an existing KYC complaint customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.
8. CDD procedure shall be followed for all joint account holders, while opening a joint account.
9. The Company can establish relationship with Politically Exposed Persons (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;
   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 will be taken at a senior level i.e. approval from HOD from Credit or Risk will have to sought in accordance with the Company's Customer Acceptance Policy.
   d) all such accounts are subjected to enhanced monitoring on an on-going basis;
   e) In case a customer or the beneficial owner of an existing account subsequently turns as a PEP, approval from HOD of Credit or Risk needs to be obtained to continue the business relationship;

   The CDD measures including enhanced monitoring on an on-going basis will be applicable to PEPs as well.

10. Enhanced due diligence process as specified in Clause 40 of the Master Directions need to be taken into consideration. Further, 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.

11. Where Company 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. Such cases should be reported to Risk team.

Note: Due diligence process as mentioned in the Operating Guidelines is to refered for dealing with request for change of (registered) mobile number for the following scenarios:

a) Where enhanced due diligence is conducted for the customers onboarded in non face to face mode and are categorised under High Risk (refer Section 40 of the KYC Master Directions) and;
b) Where accounts opened using Aadhar OTP based e-KYC in non face to face mode (refer section 17 of KYC Master Directions).

For the purpose of this section, non face to face mode shall be as specified in KYC Master Directions under section 40.

8. Reliance on third party due diligence

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship,Fedfina, may 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 daysfrom the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by Fedfina 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 customerdue 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) Fedfina will be ultimately responsible for customer due diligence and undertaking enhanced due diligence measures,as applicable.

9. Risk Management

The Company shall adopt a risk-based approach to ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. Company will adhere to the following for effective implementation of Risk Management:

a) Originals of the KYC documents shall be verified by officials of the Company and copies thereof shall be obtained and retained with the Company. Such copies shall be attested by the Company officials certifying that they have been verified with the originals.
b) KYC documents so obtained shall be properly arranged and filed in order so that they shall be available for verification any time.
c) In accordance to Section 5A of the RBI KYC Master Direction, Money Laundering and

Terrorist Financing Risk Assessment shall be carried out by Fedfina and outcome of the risk assessment exercise shall be reviewed atleast annually and placed before the Board or any committee of the Board to which power in this regard has been delegated.

10. Risk Categorisation

The Company shall categorize its customers based on the risk perceived by the Company. The level of categorisation would be Low risk, Medium Risk and High risk.

- Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- For the purpose of risk categorisation, individuals and entities whose identities and source of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Examples of low risk customers would be people belonging to lower economic strata of the society whose accounts show small balances and low turnover, government departments, government owned companies, statutory bodies, and salaried individuals.
- Customers who are likely to pose higher than average risk to the Company would be categorised as medium or high risk. While categorising the customers are medium or high risk due consideration would be given to customer's background, nature of activity, country of origin, and profile etc. In such cases, Company will apply higher due diligence measure keeping in view the risk level. Examples of customer requiring higher due diligence may include non- resident customer, trusts, societies, charitable organisation, non face to face customers, those with dubious reputations as per public information available etc. Characterisitics of High Risk and Medium Risk Customers is given as Annexure 3.
- The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
- Special care and due diligence shall be exercised in case of individuals who happen to be Politically Exposure Persons (PEP). PEP are individuals who are or have been entrusted
  with prominent public functions within or outside the country like Heads of States/Government, senior politicians, senior government/judicial/military officers, senior executive of state- owned corporations, important political party officials etc. Accounts opened under "PEP" will always be assigned with High Risk category.
- Full KYC exercise (Re-KYC) will be required to be done at least every two years for high risk individuals and entities.
- Full KYC exercise (Re-KYC) will be required to be done at least every eight years for medium risk and at least every ten years for low risk individuals and entities taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.
  If an existing KYC compliant customer desires to open another account with the Company there should no need for submission of fresh proof of identity and/or proof of address for the purpose.

11. Monitoring of Transactions:

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent logical or visible lawful purpose Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

After due diligence at the appropriate levels in the company, transactions of suspicious nature and/or any other type of transaction notified under PML Act, 2002 will be reported to the appropriate authority and a record of such transaction will be preserved and maintained for a period as prescribed in the Act.

Standard Operating Procedure (SOP) on AML is in place and it provides a detailed and elaborated process on Monitoring of transactions, Please be guided by the SOP for transaction Monitoring and other aspects on AML.

12. Beneficial Ownership

The Company shall determine the benefical ownership and controlling interest in case of the customers who are non individuals and the KYC of the beneficial owners will be sought. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice. The guidelines applicable for Beneficial Ownership is given as **Annexure II.**

13. Unique Customer Identification Code

Every customer should be provided with a Unique Customer Identification Code. This will help to identify customers, track the facilities availed, monitor financial transactions and enable the Company to have a better approach to risk profiling of customers.

14. Internal Control System

a) Internal Auditors shall ensure an independent evaluation of compliance of KYC/AML policy including legal and regulatory requirements.
b) Submission of quarterly audit notes and compliance to the Audit Committee on AML/ KYC.
c) The Company shall have an on-going employee training programme so that members of the staff are adequately trained in KYC/AML procedures.
d) The Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel called as the KYE (Know Your Employee) to ensure that persons of criminal nature/ background do not get hired/recruited.

15. Record Management

Maintenance and Preservation of records

a) maintain all necessary records of transactions between the Company 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 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) mentioned as below:

- All cash transactions of the value of more than Rs.10 lakhs or its equivalent in Indian currency, though by policy the Company does not accept cash deposits in foreign currency shall be supported by the PAN of the customer.
- PAN number to be collected by the branch for all series of cash transactions integrally connected to each other which have been valued above Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.
- All transactions involving receipts by non-profit organizations of Rs.10 lakhs or its equivalent in foreign currency.
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions.
- All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

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.

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

16. Periodic Updation (KYC in Existing Accounts)

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. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

Details pertaining to type of customers & periodic updation is appended below:

A. Individual Customers:

❖ **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 Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of the Company), letter etc

❖ **Change in address**

The Company shall have the following options for updates pertaining to 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 Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of the Company), 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.
- The Company, shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.
- Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company 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. Non- individual customers:

❖ **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 legal entity (LE) customer through its email id registered with the Company, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the Company in this regard, board resolution etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with it is accurate and shall update the same, if required, to keep it as up-to-date as possible.

❖ **Change in KYC information-**

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

C. Additional measures:

In addition to the above, the Company shall ensure that

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

ii. Customer's PAN details, if available with the Company, 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. 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 Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, the Company has the facility of periodic updation of KYC at any branch.

v. The Company shall ensure that adverse actions against the customers shall be avoided, unless warranted by specific regulatory requirements.

In case of existing customers, the Company 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 the Company 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 Company shall give the customer an accessible notice and a reasonable opportunity to be heard.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation to an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this Section. For the purpose of ceasing the operation in the account, only credits shall be allowed. Also, additional disbursement and/or top-up loans shall be ceased.

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, the Company make attempts to receive the requisite documents. The Company, at its discretion, may extend a relaxation of up to 3 months to the customer. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with the Company gives in writing to the Company that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, the Company 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.

In order to comply with PML Rules, company shall advise the customers that 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 updated document to the company within 30 days of the such update of document.

17. Introduction of New Technologies

Company 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 mechanisms, and the use of new or developing technologies for both new and preexisting products.

Further, company shall

(a) 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.

18. Prevention of Money Laundering Act, 2002 – Obligations of Company in terms of rules notified thereunder

Company has appointed "Principal Officer" who will put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. Further, with the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act, which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

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

a. issue a warning in writing; or
b. direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or
c. direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
d. by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

For the purpose of this policy document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of funds.

1. Money Laundering - Risk Perception

Following are the risks, which arise out of Money Laundering activities:

a) Reputation Risk - Risk of loss due to severe impact on reputation. This may be of particular concern given the nature of business, which requires the confidence of customers, and the general market place.

b) Compliance Risk - Risk of loss due to failure of compliance with key regulations governing the operations.

c) Operational Risk - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

d) Legal Risk - Risk of loss due to any legal action on company or its staff may face due to failure to comply with the law.

Company should ensure to cover all the above stated risks and should have proper checks to control to combat the above stated risks.

2. Maintenance of Records of Transactions and Preservation

There will be a system of maintaining proper record of transactions prescribed under PMLA, 2012 and PML Rule 2005 in prescribed format. The same along with KYC documents should be preserved for prescribed period. The Company will hire vendors where the physical copies will be preserved and also important data will be kept online on computer servers.

3. Reporting to Financial Intelligence Unit - India

Company will abide the PMLA rules for reporting information pertaining to cash and suspicious transactions to the specified authorities post conducting due enquiries. As a part of transaction monitoring mechanism, systems/ processes will be put in place to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

The Principal Officer will be responsible for submission of CTR & STR to FIU-IND. All reports have to be submitted by FEDFINA as per format prescribed by FIU-IND on FINNET portal. https://finnet.gov.in/ or as directed by FIU-IND from time to time.

4. Suspicious Transaction Monitoring and Reporting

NBFCs are required to file reports on suspicious transactions with financial intelligence unit – India (FIU), as per the prevention of Money Laundering Act (PMLA), The Suspicious Transaction Report (STR) would be furnished within 7 working days of arriving at conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The suspicious transaction is defined by RBI as a transaction, including as attempted transaction, whether or not made in cash, which to a person acting in good faith:

- 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
- Appears to be made in circumstances of unusual or unjustified complexity; or
- Appears to not have economic rational or bona – fide purpose; or
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

5. Monitoring and Reporting of Suspicious transaction activity

The Company will keep a continuous vigil with regards to customers behaviour or approach while dealing with the company. The company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose.

In case any usual act or event or behaviour is noticed in relation to customer, the same shall be investigated and if required report as suspicious activity. The staff of branches / department should observe the traits of customer that raise suspicion. List of suspicious transactions to be tracked is given below:

- Reluctance on part of the customer to provide confirmation regarding his identity, nature of business, business relationship, officers or directors or its locations
- KYC documents provided by the customer are forged, fabricated or altered
- KYC documents provided by the customer cannot be verified (e.g foreign documents)
- Forged documents provided by the customer (e.g. fake title deeds)
- Difficulty in identifying beneficial owner of the transaction
- Nature of transaction under taken by the customer is too complex or the customer is not able to explain the source of funds
- Nature of transaction undertaken by the customer does not justify his nature of business or lifestyle or standard of living
- Customer has limited or no knowledge about the money involved in transaction or conducting transaction on behalf of someone else
- Customer is investigated for criminal offence by law enforcement agency
- Customer is investigated for terrorist financing or terrorist activities

- Adverse media report about the customer
- Negative Information about the customer received from any other financial institution (e.g. fraud etc)
- For all part prepayments/ foreclosures which are not balance transfer (BT) involving Rs. 0.50 Crs. or above should be reviewed through customer service and reported to Principal Officer. The Risk team shall review whether same is suspicious or not and accordingly Principal Officer shall report the same if required.
- Any enquiry from CBI, Police, Enforcement Directorate, Department or Vigilance and Anti-corruption, Income Tax or Service tax authorities etc about the statement of account of the customer should result in STR.

6. Monitoring and Reporting of Cash Transactions

No cash of Rs. 50,000/- and above shall be accepted from a Customer/ any other intermediary (auction cases) without obtaining a copy of the PAN card of the Customer/any other intermediary. In case a Customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

Further, maximum cash limit for acceptance and disbursement shall be in line with the extant regulatory guidelines and Income Tax guidelines u/s 269SS, 269ST and 269T (as amended from time to time).

Any cash transactions of Rs. 10 lakhs and above and integrally connected cash transactions of Rs, 10 lakh and above per month shall be reported to FIU-IND by 15th of the succeeding month as CTR.

The Company shall lay down proper mechanism to check any kind of attempts to avoid disclosure of PAN details. In case of possible attempts to circumvent the requirements, the same shall be reviewed from the angle of suspicious activities and shall be reported to FIU-IND, if required.

19. Central KYC Records Registry

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.

In terms of provision of Rule 9(1A) of PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer. The Company 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 Company 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. Once KYC Identifier is generated by CKYCR, REs shall ensure that the same is communicated to the individual/LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to April 1, 2017 and April 1, 2021 respectively at the time of periodic updation as specified in the Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard. Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company 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 –

a. there is a change in the information of the customer as existing in the records of CKYCR;
b. the current address of the customer is required to be verified;
c. the RE 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.
d. the validity period of documents downloaded from CKYCR has lapsed

20. Combating Financing of Terrorism

Fedfina shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND)on priority.
As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Reserve Bank of India, Fedfina ensures to update the consolidated list of individuals and entities in its de-dupe process.

21. Offences Constituting Money Laundering

As per 2(1)(y) of the Prevention of Money Laundering Act, 2002, Scheduled offence means the offences specified under Part A of the Schedule; or the offences specified under Part B of the Schedule if the total value involved in such offences is one crore rupees or more; or the offences specified under Part C of the Schedule;

The Schedule to the Prevention of Money Laundering Act, 2002 lists offences under the Indian Penal Code, the Narcotic Drugs and Psychotropic Substances Act, 1985, Explosive Substances Act, 1908, The Unlawful Activities (Prevention) Act, 1967, the Prevention of Corruption Act, 1988, The Customs Act, 1962 etc. The detailed list can be accessed from the PML Act, 2002.

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

Company shall ensure meticulous compliance section 52 of Master Directions along with with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" as specified in laid down in Annex III of the Master Direction.

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

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

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 AlQaida 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.html

Company 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 43 (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 the 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.

24. Annexures

Annexure I - Indicative list of documents for Customer Due Diligence (CDD)

Sr. No.	Individual / Type of Entity (features to be verified)	Documents required
1.	Individuals	Permanent Account Number (Mandatory) (the same shall be verified from the verification facility of the issuing authority including through DigiLocker) AND Any one of the OVD (Proof of Identity and Address) AND One recent photograph **List of OVD:** i. the passport, ii. the driving licence, iii. Proof of possession of Aadhaar number, iv. the Voter's Identity Card issued by the Election Commission of India, v. Job card issued by NREGA duly signed by an officer of the State Government and vi. Letter issued by the National Population Register containing details of name and address. 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. 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. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:- i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. Property or Municipal tax receipt; iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public

		sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; Customer shall submit OVD with current address within a period of three months of submitting the documents specified above.
2.	**Proprietorship Concerns**	Documents or equivalent e-documents which could be obtained as proof of business/activity for proprietary firms (any two) in additions to the documents of the proprietor as individual: (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) GST certificate (provisional / final) (e) Certificate /registration document issued by Sales 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 the Company is satisfied that it is not possible to furnish two such documents, it may, at their discretion, accept only one of those documents as proof of business/activity. Provided that it undertakes contact point verification and collects 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.
3.	**Company** Name of the Company Principal place of business Mailing Address, Telephone No.	Certified copies of following documents or equivalent e-documents should 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. Individual KYC of person authorised to transact on behalf of the company

		(e) Documents as specified for individuals (KYC) 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) the names of the relevant persons holding senior management position; and (g) the registered office and the principal place of its business, if it is different
4.	**Partnership Firms** Legal Name Addr ess Names of all partners and their address Telephone No.	Certified copies of following documents or equivalent e- documents should be obtained: (a) Registration certificate (b) Partnership deed (c) Permanent Account Number of the partnership firm (d) Documents as specified for Individual (KYC), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf (e) the names of all the partners and (f) address of the registered office, and the principal place of its business, if it is different.
5.	**Trust** Name of Trust / Trustees / Settlors / beneficiaries / Signatories / founders Telephone No.	Certified copies of following documents or equivalent e- documents should be obtained: (a) Registration certificate (b) Trust deed (c) Permanent Account Number or Form No.60 of the trust (d) Documents as specified for Individual (KYC), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf (e) the names of the beneficiaries, trustees, settlor and authors of the trust (f) the address of the registered office of the trust; and (g) list of trustees and documents as specified for individuals (KYC), for those discharging the role as trustee and authorised to transact on behalf of the trust.
6.	**Unincorporated Association / Body of Individuals (Includes Unregistered Trusts/ Partnership Firm s / Societies)**	Certified copies of following documents or equivalent e-documents should 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) Individual KYC of person authorised to transact on behalf of the firm (e) Any other information/document as may be required to collectively establish the legal existence of such an association or body of individuals.

7.	**Others**	For opening accounts of juridical persons 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 equivalent e-documents shall be obtained: (a) Document showing name of the person authorised to act on behalf of the entity; (b) Individual KYC of person authorised to transact on its behalf (c) Any other information/document as may be required to establish the legal existence of such an entity/juridical person

Annexure II – Beneficial Owners

Sr. No.	Applicable for	Guidelines	
1.	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.	"Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements
2.	Partnership Firm	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 % of capital or profits of the partnership.	
3.	unincorporated association or body of individuals	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 % of the property or capital or profits of the unincorporated association or body of individuals.	
4.	Where no natural person is identified under (1), (2) or (3) above	beneficial owner is the relevant natural person who holds the position of senior managing official.	
5.	Trust/ nominee or fiduciary accounts	identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.	

		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.
6.	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 companies.

Annexure III – Characteristics of High Risk Customer and Medium Risk Customers

Characteristics of High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations;
4. Customers with dubious reputation as per public information available or commercially available watch lists;
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
7. Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
8. Non face-to-face customers;
9. High net worth individuals;
10. Firms with 'sleeping partners' ;
11. Companies having close family shareholding or beneficial ownership ;
12. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
13. Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low level staff does not constitute physical presence;
14. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the NBFC;
15. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc;

16. Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;
17. Gambling/gaming including "Junket Operators" arranging gambling tours;
18. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);
19. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;
20. Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
21. Customers that may appear to be Multi level marketing companies etc.

Characteristics of Medium Risk Customers

1. Stock brokerage;
2. Import / Export;
3. Gas Station;
4. Car / Boat / Plane Dealership;
5. Electronics (wholesale);
6. Travel agency;
7. Telemarketers; Providers of telecommunications service, internet café, IDD call service, phone

Annexure IV – Standards with respect to undertaking Video – Customer Identification Process (V-CIP)

1. V-CIP Infrastructure

a. The Company shall comply 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 shall be housed in the Company's own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines.

b. 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

c. The Company 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 shall be recorded in an auditable and alteration proof manner.

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

e. The video recordings shall 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.

f. 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 shall rest with the Company. Appropriate artificial intelligence (AI) technology may be used to ensure that the V-CIP is robust.

g. 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.

h. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

2. **V-CIP Procedure**

- The Company 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 Company specially trained for this purpose. The official shall be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it
- 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.
- 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.
- Any prompting, observed at end of customer shall lead to rejection of the account opening process.
- 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 shall be factored in at appropriate stage of work flow.
- The authorised official of the Company 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:
  i. OTP based Aadhaar e-KYC authentication
  ii. Offline Verification of Aadhaar for identification
  iii. KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer
  iv. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker
- The Company shall ensure to redact or blackout the Aadhaar number as per the relevant regulatory guidelines.
- In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

- Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.
- 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.
- The Company 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.
- Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
- The authorised official of the Company 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.
- Assisted V-CIP shall be permissible when the Company takes help of Banking Correspondents (BCs) facilitating the process only at the customer end. The Company 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 Company.
- 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.
- All matters as required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

3. V-CIP Records and Data Management

j. The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs 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 the KYC-AML Master Direction, shall also be applicable for V- CIP.

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