POLICY ON KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML)

WALKfin
we invest in future

Content of the Policy

1. Introduction 3
2. Objective & Applicability 3
3. Definition 3
4. Compliance of KYC policy 5
5. Key Elements of the policy 5
6. Customer Acceptance Policy (CAP) 5
7. Risk Management 6
8. Customer Identification Procedure (CIP) 7
9. Identification of Beneficial Owner 11
10. Customer Due Diligence (CDD) 12
11. V-CIP 13
12. On-going Due Diligence/Periodic Updation 13
13. Enhanced Due Diligence 14
14. Record Management and Retention 15
15. Reporting Requirements to Financial Intelligence Unit - India 16
16. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) 16
17. Unique Customer Identification Code (UCIC) 17
18. Selling of Third-Party Products 17
19. Appointment of designated Director and Principal Officer 17
20. Hiring of Employees and Employee training 17

Annex – I Digital KYC Process 18

Annex – II: Video Based KYC process (V-CIP) 20

KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML) POLICY (Version 3)

Introduction

The Prevention of Money Laundering Act, 2002 (PML) is enacted to prevent and control money laundering and to confiscate and seize the property obtained from the laundered money. The PML Act and Rules notified thereunder, came into effect from 1st July, 2005.

The Reserve Bank of India ("RBI") has issued/amended guidelines on Know Your Customer (KYC) and Anti-money Laundering (AML) standards from time to time to be followed by all the regulated entities and has advised all regulated entities to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

Accordingly, in compliance with the RBI Master Direction 2016 issued by RBI and amended from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company. This policy is applicable to all categories of products and services offered by the Company.

Objective & Applicability

The primary objective is to prevent the Company from being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines mandate the Company to determine the true identity and beneficial ownership of accounts, source of funds, the nature of the customer's business, the reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

The policy is applicable across all branches and all product/business segments of the Company. All departments shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

Definition

i. **Beneficial Owner (BO)** shall mean 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.
ii. **Customer** means a person who is engaged in a financial transaction or activity with a Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
iii. **Obtaining a certified copy** 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 authorized officer of the Company.

iv. **Digital KYC** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Company.

v. **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.

vi. **Officially Valid Document (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

vii. **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)

viii. **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:

- ✓ 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 rationale or bona-fide purpose; or
- ✓ gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

ix. **Video based Customer Identification Process (V-CIP)** mean an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company 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.

All other expressions, unless defined herein, shall have the same meaning as have been assigned to them in the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and RBI's Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time.

Compliance of KYC policy:

The Company shall take adequate measures to ensure compliance with KYC guidelines.

Key Elements of the policy

The Company is hereunder framing the KYC policy incorporating the following four key elements:

i. Customer Acceptance Policy ("CAP")
ii. Risk Management
iii. Customer Identification Procedures ("CIP") and
iv. Monitoring of Transactions

Customer Acceptance Policy (CAP)

The company shall follow the following norms while accepting, dealing and taking the decision to grant any credit facility to customers who approach the Company for availing financial assistance.

The Company will:

i. Not open an account in an anonymous fictitious / benami name or where its unable to do customer due diligence (CDD) on account of non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.
ii. Carry out full-scale customer due diligence (CDD) for all customers before opening an account.
iii. Obtain/sought mandatory KYC documents and other information from the customer while opening an account and during the periodic updation, is specified. Obtained explicit consent for taking optional/additional information after the account is opened.
iv. Undertake the CDD procedure at the Unique Customer Identification Code (UCIC) level, thus, if an existing KYC compliant customer desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
v. put in place a suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
vi. The Company shall clearly spell out a circumstance in which a customer is permitted to act on behalf of another person/entity.
vii. Verify the PAN obtained from the customer from the verification facility of the issuing authority.

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

ix. When the identity of the account holder is not known, the Company shall file suspicious Transaction Reporting (STR).

x. Photocopies of documents submitted by the clients shall be compulsorily verified with original, with signature/confirmation of the person verifying shall be put as proof verification

Risk Management

For Risk Management, the Company will have a risk-based approach which includes the following;

All the customers are categorized into low, medium and high risk based on their profile. The risk categorization can be done based on the assessment and risk perception of the Company.

The risk categorization will be undertaken based on the following parameters:

- Customer's identity,
- Social/financial status,
- Nature of business activity, and
- Customer business information and their location etc.
- Ability of the customers to confirm identity documents through online or other services offered by issuing authorities.

Where businesses believe that a particular customer falling under a category mentioned above is in his judgment falling in a different category, he may categorize the customer, so long as appropriate justification is provided in the customer file.

As per the Company product profile /loan ticket size and type of customer with which we deal with, most of our customers will be of low-risk profile given the nature of its business.

Indicative List of Risk Categorization

I. Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of income/fund can be easily identified and transactions in whose accounts by and large conform to the known profile and not covered in any of the below two categories, shall be categorized as low risk.

The MSME enterprise are entities of modest mean and lie at the bottom of the economic or into non-formal sector. The most of their turnover might be conducted in cash. However, for PML and AML purview the same shall be categories in low risk due to the small aggregate transaction.

Illustrative examples of low risk:

- ✓ salaried employees whose salary structures are well defined
- ✓ people belonging to lower economic strata of the society whose accounts show small balances and low turnover.

II. Medium & High-Risk Category

Customers who are likely to pose a higher than average risk may be categorized as medium or high risk depending on the customer's background, nature and location of the activity, country of origin, sources of funds and client profile etc.

Illustrative examples of medium and high risk

- ✓ Non-Resident Customers.
- ✓ High Net worth Individuals
- ✓ Trust, NGOs and organizations receiving donations
- ✓ Politically Exposed Persons (PEPs)
- ✓ Persons having dubious reputation as per public information available, etc.
- ✓ Firms with 'sleeping partners',
- ✓ Customers requesting for frequent change of address/contact details
- ✓ Sudden change in the loan account activity of the customers
- ✓ Frequent closure and opening of loan accounts by the customers

The Company shall undertake ongoing due diligence and monitoring of high-risk customers to ensure that their transactions are consistent with Company knowledge.

Money Laundering and Terrorist Financing Risk Assessment:

Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise should be carried out annually to identify, assess and take effective measures to mitigate the money laundering and terrorist financing risk arising from clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The risk assessment should be commensurate to size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment approach should also take cognizance of the overall sector-specific vulnerabilities, if any, that RBI may share time to time.

Risk Based Approach (RBA) should be applied for mitigation and management of risks identified and Board approved policies, controls and procedures in vogue should be accordingly aligned.

Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent sources of documents, data or information to ensure that the customer is not a fictitious person.

The Company will undertake CIP while establishing a relationship, carrying out any financial transaction, when there is a doubt about the authenticity or adequacy of identification data already obtained while selling third party products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000 and where the customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000.

1. The nature of information/documents to be obtained from the customer will depend on the type of customer (individual, corporate etc.)

   i. When Customers are natural person:
      - ✓ Address/location details
      - ✓ Identity Proof and Recent photograph of all customers

   ii. Customers that are legal persons:

      - ✓ Legal status of the legal person/entity through proper and relevant documents.
      - ✓ Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified.
      - ✓ Understand the ownership and control structure of the customer and determine who are the natural persons and ultimately control the legal person.

2. The company shall obtain the following information/documents or equivalent e-documents from the customer while establishing an account-based relationship:

Type of Customers	Documents or the equivalent e-documents
Individual Identification and address proof	Any two of the following documents (PAN being mandatory) 1. Passport 2. PAN Card/Form 60 3. Aadhaar Card 4. Voter's Identity Card issued by Election Commission 5. Driving License 6. 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. Where the above-mentioned documents do 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 and submit OVD with current address within period of three months:

Type of Customers	Documents or the equivalent e-documents
	I. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); II. property or Municipal tax receipt; III. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; IV. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;
Proprietary firms Proof of business/ activity	In addition to the above, any two of the following documents or the equivalent e-documents i. Registration certificate ii. Certificate/license issued by the municipal authorities under Shop and Establishment Act. iii. Sales and income tax returns. iv. CST/VAT/ GST certificate (provisional/final). v. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. vii. Complete Income Tax Return (not just the acknowledgment) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. viii. Utility bills such as electricity, water, landline telephone bills, etc. In case Company is satisfied that it is not possible to furnish two such documents, Company may, at their discretion, accept only one of those documents as proof of business/activity. Such other documents in respect of nature of business and financial status of an entity.
Partnership Firm	Certified copy of all the below documents or the equivalent e-documents thereof; I. Registration certificate

Type of Customers	Documents or the equivalent e-documents
	II. Partnership deed III. Permanent Account Number of the partnership firm and along with partners PAN, Aadhaar Card, Passport or any of OVD documents. IV. Such other documents in respect of nature of business and financial status of an entity.
Legal Entity	Certified copy (by Director/CS) of all the below documents or the equivalent e-documents thereof I. Certificate of incorporation II. Memorandum and Articles of Association (MoA and AoA) III. PAN IV. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their PAN, Aadhaar Card, Passport or any of OVD documents. V. Such other documents in respect of nature of business and financial status of an entity.
Trust	Certified copy of all the below documents or the equivalent e-documents thereof; I. Registration certificate II. Trust deed III. Permanent Account Number or Form No.60 of the trust and along with signatories PAN, Aadhaar Card, Passport or any of OVD documents. IV. Such other documents in respect of nature of business and financial status of an entity.
Unincorporated association/ Unregistered trusts/partnership firms or a body of individuals	Certified copy of all the below documents or the equivalent e-documents thereof; I. Resolution of the managing body of such association or body of individuals II. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals III. Power of attorney granted to transact on its behalf and PAN of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons. IV. Such other documents in respect of nature of business and financial status of an entity.
Juridical persons not specifically covered such as societies, universities and local bodies like	Certified copy of all the below documents or the equivalent e-documents thereof; I. Document showing name of the person authorised to act on behalf of the entity;

Type of Customers	Documents or the equivalent e-documents
village panchayats	II. Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and III. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person. IV. Such other documents in respect of nature of business and financial status of an entity

The company may accept such other documents from the customer in addition to above-mentioned documents to satisfy and establish the legal existence of such an entity/person. Such a list of documents shall be approved by the Head of -Operations.

Identification of Beneficial Owner

Before opening an account of a legal person who is not a natural person (i.e., non-individual), the Company shall identify the beneficial owner(s) and verify the beneficial owner's identity.

Nature of Entity	Beneficial Owner of the Entity	
Company	the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.	Controlling ownership interest" means ownership of or entitlement to more than 25% of shares or capital or profits of the company; "Control" shall include the right to appoint the 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;
where the client 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,	Ownership of entitlement to more than 15% of capital or profits of the partnership;
where the client 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	ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals
where no natural person is identified	the beneficial owner is the relevant natural person who holds the position of senior managing official;	

Nature of Entity	Beneficial Owner of the Entity
where the client is a trust	the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership
Where the client or the owner of the controlling interest is an entity listed on a stock exchange or 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.

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 will be obtained.

Customer Due Diligence (CDD)

For undertaking CDD, either of the following should be obtained from an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

Sr. No	Nature of Documents	Type of Verification
1.	Proof of possession of Aadhaar number where offline verification can be carried out	The Company shall carry out offline verification.
2.	Proof of possession of Aadhaar number where offline verification cannot be carried out.	The Company shall carry out verification through digital KYC as specified under Annex I.
3.	Any OVD containing the details of identity and address.	The Company shall carry out verification through digital KYC as specified under Annex I.
4.	Any equivalent e-document of any OVD containing the details of identity and address.	The Company 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

Provided that for a period not beyond such date as may be notified by the Government for the NBFC, instead of carrying out digital KYC, the Company 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.

The Company may rely on the customer due diligence done by third party for the purpose of verifying the identity of customers (CIP) for commencement of an account-based relationship. The Company shall adhere to the following conditions that the;

- ✓ Records or the information of the customer due diligence will be obtained within two days from the third party or from the Central KYC Records Registry.
- ✓ copies of identification data and other relevant documentation relating to the customer will be made available from the third party upon request without delay.
- ✓ third party will be 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.
- ✓ third party shall not be based in a country or jurisdiction assessed as high risk.
- ✓ ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures will be responsibility of the Company.

V- CIP

The Company may use V-CIP as per Annex- II to carry out:

- ✓ On-boarding for individual customers,
- ✓ Proprietor in case of proprietorship firm,
- ✓ Authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
- ✓ Updation/Periodic updation of KYC for eligible customers

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.

On-going Due Diligence/Periodic Updation:

The Company will adopt a risk-based approach for periodic updation of KYC. The periodic updation will 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.

Entity	Criteria	Documents for periodic updation.
Individual	No change in KYC information	a self-declaration will be obtained through

Customers		registered email id, mobile number or letter.
	Change in address	a self-declaration of the new address will be obtained through registered email id, mobile number or letter 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. or a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address
Other than Individual	No change in KYC information	a self-declaration will be obtained through registered email id, letter from an official authorised along with Board resolution. The Company shall also obtain fresh Beneficial Owner (BO) information and update the record.
	Change in address	The company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

In addition to above, Company shall ensure that

- ✓ If KYC documents is not as per current CDD standard, then the KYC documents of the customer is as per the current CDD standards shall be obtained, even if there is no change in the customer information.
- ✓ PAN details shall be verified from the database of the issuing authority at the time of periodic updation of KYC
- ✓ Company shall provide an acknowledgment for receipt of any documents/letter for KYC updation and the record shall be promptly updated in the system mentioning the date of KYC updation.

Enhanced Due Diligence

The Company is primarily engaged in MSME finance. It does not deal with such category of customers who could pose a potentially high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny.

- ➢ Accounts of non-face-to-face customers

The Company will ensure that the first payment is to be effected through the customer's KYC-complied account maintained with another regulated entity, for enhanced due diligence of non-face-to-face customers.

- Accounts of Politically Exposed Persons (PEPs)

If the customer or beneficial owner is a Politically Exposed Persons, the Company shall ensure that;

- ✓ sufficient information including information about the sources of funds and accounts of family members and close relatives is undertaken wherever possible;
- ✓ the identity of the person shall have been verified before accepting the PEP as a customer;
- ✓ the decision to open an account for a PEP will be considered at a committee or board level
- ✓ all PEP accounts will be subjected to enhanced monitoring on an ongoing basis;
- ✓ in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, committee or board level approval is obtained to continue the business relationship;

Record Management and Retention

The Company shall take the following steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules:

- The Company shall maintain all records of the transaction between the Company and the customer for at least 5 years from the date of the transaction.
- The company shall preserve the identification/address documents of the customer for a period of 5 years after the business relationship is ended.
- The Company will 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.
- The Company shall maintain all the information and a record of transactions as prescribed under in Prevention of money laundering rule 3 including the following:
  - the nature of the transactions;
  - the amount of the transaction and the currency in which it was denominated;
  - the date on which the transaction was conducted; and
  - the parties to the transaction.

Maintenance of records of transactions (nature and value) as per Rule 3 of PML (Maintenance of Records) Rules 2005**:**

a) All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.

b) All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.

c) All transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency

d) 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.
e) All suspicious transactions whether or not made in cash.
f) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.
h) Receipt of Rs. 2 Lakhs or more in cash from a person in single day or in respect to single transactions as per section 269ST of Income Tax, 1961.

The Company shall maintain records of the identity and address of their customer, and records in respect of the above transactions in hard or soft format.

Reporting Requirements to Financial Intelligence Unit - India

The Company will be furnished to the Director, Financial Intelligence Unit-India (FIU-IND), information referred above as per Rule 7 of the PML (Maintenance of Records) Rules, 2005.

- ✓ The Principal Officer of the Company will furnish the cash transaction report (CTR) in prescribed format in respect to transaction referred clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 by 15th of every succeeding month.
- ✓ The Principal Officer of the Company will furnish the Suspicious Transaction Report in prescribed format in respect to transaction referred in clause (D) of sub-rule (1) of rule 3 within 7 working days after arriving at conclusion that the transaction is suspicious.
- ✓ The Principal Officer of the Company will furnish the information in prescribed format in respect to transaction clause (F) of sub-rule (1) of rule 3, 15th of the every succeeding the quarter.
- ✓ The Company shall deploy robust software which are capable (i) of throwing alerts when the transactions are inconsistent with risk categorization, (ii) updated profile of the customers will be put in to use as a part of effective identification and reporting of suspicious transactions.

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

The Company will capture customer KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship as per KYC templates for 'Individuals' and 'Legal Entities' (LEs) issued by CERSAI.

Once KYC Identifier is generated by CKYCR, Company will communicate the same to the individual/LE.

In case the customer submit the KYC Identifier for establishing an account-based relationship than Company will obtain explicit consent from the customer to download/retrieve records from the CKYCR using the KYC identifier. The customer will not be required to submit the same KYC record or information unless;

- ✓ there is a change in the information of the customer as existing in the records of CKYCR;
- ✓ the current address of the customer is required to be verified;
- ✓ the Company 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.

Unique Customer Identification Code (UCIC)

Every customer is provided with a unique customer ID. This helps to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the organization to have a better approach to risk profiling of customers.

Selling of Third-Party Products

The Company acting as agents while selling third party products shall comply with the following direction;

- ✓ If transaction value is above Rs. 50,000, the identity and address of the walk-in customer will be verified by the Company.
- ✓ The Company shall maintain complete records of the third-party product.
- ✓ The Company shall obtain and verify the PAN given by the account-based as well as walk-in customers.

Appointment of designated Director and Principal Officer:

Mr. Pravash Dash Managing Director & CEO will be the designated director who is responsible for ensuring overall compliance as required under PML Act and the rules.

Mr. Kunal Mehta, Executive Director designated as Principal Officer who shall be responsible for monitoring and reporting of all transactions and sharing of information to FIU-IND.

Senior Management shall be defined as per the HR policy of the Company

Hiring of Employees and Employee training

The Company shall undertake adequate screening mechanism as an integral part of their personnel recruitment/hiring process and conduct on-going employee training programme that the employees are adequately trained in KYC/AML policy.

Annex – I Digital KYC Process

The Company will made available digital KYC application (apps/software) at customer touch points for undertaking KYC of the customers. The same should be undertaken only through authenticated application of the Company.

The access of the application will be controlled by the Company and shall not be used by unauthorized persons. The access of the application will be only through login-id and password or Live OTP or Time OTP controlled mechanism given to authorized officials.

For KYC the customer should visit the Company office/branch or location of the authorized official or vice-versa. The original OVD should be in possession of the customer.

Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in the Customer Application Form (CAF). The application should add a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee code and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

The application should 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.

Live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out should be placed horizontally and should be captured vertically from above and water-marking in readable form as mentioned in above point.

No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

The live photograph of the customer and original documents should be captured in proper light such that its clearly readable and identifiable.

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 may be auto-populated by scanning the QR code instead of manual filing the details.

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. In case 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 no case the mobile number of authorized officers shall not be used for customer signature. The Company should ensure that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

Authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. The authorized official should be verified with One Time Password (OTP) which should be sent to his/her mobile registered number. Upon successful OTP validation, it should 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. Subsequent to all these activities, the Application should give information about the completion of the process and submission of activation request to activation officer and generate the transaction-id/reference-id number of the process.

The authorized officer should intimate the details regarding transaction-id/reference-id number to customer for future reference.

The authorized officer should 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.

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

Annex – II: Video Based KYC process (V-CIP):

a) V-CIP Infrastructure

i. The technology infrastructure for V-CIP shall be housed in the Company own premises and the V-CIP connection and interaction should be originate from the Company own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii. The Company infrastructure should 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 should be adequate to allow identification of the customer beyond doubt.

v. The application should 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 RE. 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 should be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii. The V-CIP infrastructure should 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.

viii. The V-CIP application software and relevant APIs / webservices should 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. The Company should formulate a clear work flow and standard operating procedure for V-CIP. The V-CIP process should be operated only by specially trained officials of the Company.

ii. In case there is a disruption in the process, the same should be aborted and a fresh session to be initiated.

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

iv. If any prompting is observed at end of the customer, the application should reject the process of KYC.

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 the appropriate stage of workflow.

vi. The authorized official of the Company who is performing the V-CIP should 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.

✓ In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the Company should ensure that the XML file or QR code generation date should not be older than 3 days from the date of carrying out V-CIP.

✓ The Company should also complete the V-CIP within 3 days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document.

vii. In case the address of the customer is different from that indicated in the OVD, suitable records of the current address should be captured. The Company should also ensure that the economic and financial profile/information submitted by the customer should also confirmed from the customer undertaking the V-CIP in a suitable manner.

viii. Application should capture a clear image of PAN card displayed by the customer during the process, except where e-PAN is provided by the customer. The PAN details should be verified from the database of the issuing authority including through Digilocker.

ix. The Company should ensure that use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

x. The authorized official of the Company should 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 should match with the details provided by the customer.

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

c) V-CIP Records and Data Management

i. The entire data and recordings of V-CIP should be stored in a system / system located in India. The Company should 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 RBI master direction shall be equally applicable for V-CIP.

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