

ASIRVAD MICROFINANCE LIMITED

KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY LAUNDERING POLICY

Approval Details:

Approval Date	25 th Jan 2021
Effective Date	25 th Jan 2021
Approved by	Board of Directors
Version	Version 0.3
Policy Owner	Chief Operating Officer
Next Review/ Amendment Date	7 th August 2023

1. INTRODUCTION.....	3
2. POLICY STATEMENT	3
3. OBJECTIVES OF THE POLICY:	3
4. SCOPE OF THE POLICY	3
5. IMPORATANT DEFINITIONS.....	4
6. KEY ELEMENTS OF THE POLICY	6
6.1 CUSTOMER ACCEPTANCE POLICY (CAP)	6
6.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP)	7
6.2.1. Customer Due Diligence procedure (CDD) in case of individuals	8
6.2.2. Verification of equivalent e-document:	8
6.2.4 .Identification of beneficial owner.....	9
6.2.5 .CDD measures in respect of non-individuals:	9
6.2.6 .Facilitating third party products.....	9
6.3 RISK MANAGEMENT.....	10
6.4. MONITORING OF TRANSACTIONS.....	10
6.4.1. Ongoing due diligence	10
6.4.2. Periodic updation	11
6.4.3. KYC updation for existing customers	12
7. A.ENHANCED DUE DILIGENCE.....	12
8. CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS	15
9. MAINTENANCE OF RECORDS OF TRANSACTIONS	15
10. GENERAL.....	16
10.1.Adherence to KYC guidelines by agents.....	16
10.2 Principal Officer.....	16
10.3 Designated Director	16
10.4 CDD Procedure and sharing KYC information with central KYC records Registry (CKYCR)	16
10.5 Training Program	16
11. COMPLIANCE OF KYC POLICY	17
12. Non-Individuals (Companies, Firms, Trusts etc.)	17

1. INTRODUCTION

In accordance with the KYC Master Directions issued and amended from time to time by Reserve Bank of India (RBI) all Regulated Entities (REs) including AMFL are required to put in place policy and procedures on customer onboarding and monitoring of transactions according to the terms and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India. Accordingly, AMFL puts in place the policy as detailed below.

2. POLICY STATEMENT

AMFL is primarily engaged in Microfinance and by nature of its business and exposure size the potential risks of money laundering, terrorist financing that it poses is relatively very low. AMFL recognizes the importance of the Anti-Money Laundering (AML) programs and commits itself to introducing a vigilant culture in preventing money laundering to the extent applicable to the firm. Accordingly puts in place a detailed KYC & AML policy and procedures hereunder in line with RBI Directions and Prevention of the Money Laundering Act/Rules as amended from time to time.

3. OBJECTIVES OF THE POLICY:

The policy is framed to ensure the following

- To provide a framework on threats of money laundering while dealing with the customers.
- To protect the company from being used for criminal activities and money laundering.
- To ensure that the staff are aware about the KYC/AML norms applicable to the business and to ensure the proper training on the same.
- To create an effective system for customer onboarding and on the monitoring transactions which helps to understand the risk associated with each customer.
- To ensure the proper reporting of incidents which are comes under the purview of money laundering act.
- To define the roles and responsibilities for ensuring the compliance.
- To ensure the updates/review of KYC/AML standards according to the applicable laws and regulatory guidelines.

4. SCOPE OF THE POLICY

This Policy applicable to all employees of AMFL and third-party vendors engaged with AMFL. The Policy is framed with necessary procedures to enable the Company to comply with its legal obligations.

This Policy is mainly framed to cover the money laundering risk associated with the below mentioned products and to fix the responsibilities over the employees who are dealing with the customers and third-party vendors. The policy aims to meet the legal requirements according to the depth of risks that AMFL is exposed to in respect of the businesses/activities (business verticals) being undertaken by the company as detailed below.

- Microfinance
- MSME
- Gold Loan
- Other loans

- Third party products

The policy also aims to make all employees aware of their responsibilities and the consequences of non-compliance with this policy.

5. IMPORATANT DEFINITIONS

(i) **Beneficial Owner (BO)**

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

“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 a 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.

- b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than **15 per cent** of capital or profits of the partnership.
- c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than **15 per cent** of the property or capital or profits of the unincorporated association or body of individuals.

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

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

- (ii) **“Central KYC Records Registry” (CKYCR)** means an entity defined under Rule 2(1) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

(iii) **“Customer “means.**

- a. a person who is engaged in a financial transaction or activity with AMFL and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.
- b. any other person connected with a financial transaction which can pose significant reputation or other risks to AMFL.

- (iv) **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and

- the beneficial owner.
- (v) **“Digital KYC”** means 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 Regulated Entity (RE) as per the provisions contained in the Act.
- (vi) **“Digital Signature”** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- (vii) **“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.
- (viii) **“Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- (ix) **“Non-face-to-face customers”** means customers who open accounts without visiting branches / offices of AMFL or meeting its officials.
- “Obtaining certified copy of Officially Valid Document (OVD)” – Means comparing the copy of OVD with the original and recording the same on the copy by authorized officer of AMFL.
Certified OVD shall also contain the customer id number and shall be filed carefully for future verification.
- (x) **“Offline verification”** means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as per clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
- (xi) **“Senior Management”** for the purpose of the policy shall constitute MD, CRO, COO, CCO.
- (xii) **“Video based Customer Identification Process (V-CIP)”**: an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, **live**, informed consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification **and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.**
- (xiii) **“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/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- (xiv) **“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.
- (xv) **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for Asirvad Customers.
- (xvi) **“Regulated Entity” (RE)** for the purpose of this Policy would mean the Company regulated by RBI.
- (xvii) **“Walk-in Customer”** means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
- (xviii) **Group** – The term “group” shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).
- (xix) **Non-profit organisations” (NPO)** means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

6. KEY ELEMENTS OF THE POLICY

As mentioned, this policy is applicable to all business operations and services and to the business verticals of AMFL. The policy will be supported by necessary operational guidelines issued from time to time.

The essential procedures forming part of KYC/AML Policy are stated below.

1. Customer Acceptance Policy (CAP)
2. Customer Identification Procedures (CIP)
3. Risk Management (Risk Categorization)
4. Monitoring of Transactions (including Reporting STR, CTR & CCR) & Ongoing Monitoring.

6.1 CUSTOMER ACCEPTANCE POLICY (CAP)

AMFL’s CAP lays down criteria for acceptance of customers. While taking decision to grant any facilities to the customers as well as during the continuation of any facilities the following norms and procedures will be followed by the company

- a. No account will be opened in anonymous or fictitious/benami name.
- b. No account is opened where the AMFL is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- c. No transaction or account-based relationship will be undertaken without following the Customer Due Diligence procedure (CDD).
- d. Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done before opening a new account to ensure that the identity of the Customer does not match with any person with known

- criminal background or with banned entities.
- e. A Unique Customer Identification Code (UCIC) shall be allotted to new and existing customers. AMFL shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of AMFL desires to open another account with AMFL, there shall be no need for a fresh CDD exercise.
 - f. AMFL has a system in place 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
 - g. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.
 - h. Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
 - i. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
 - j. Where AMFL is suspicious 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.

6.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer Identification involves verification of customer's identity by using reliable, independent source documents, data, or information. AMFL shall obtain enough information necessary to verify the identity of each Customer. A broad guideline for the customer identification is given below:

AMFL shall undertake identification of customers in the following cases,

- a. an account-based relationship is being established.
- b. there is doubt about the authenticity or adequacy of customer identification data already obtained.
- c. facilitating products for their party vendors, for more than Rs. 50,000/-.
- d. carrying out transactions with walk in customers, where the amount involves equal or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
- e. AMFL has reasons to believe that a customer is intentionally structuring transactions into a series of transactions below the threshold of Rs. 50,000/-.

In all situations, AMFL will conduct mobile number authentication by way of OTP and bank account will be verified before initiating a payment. Geotagging will be used in situations performing field verification.

As a progressive organization AMFL will introduce V-CIP (Annexure II) and Digital KYC (Annexure III) to ensure the CDD procedures at all situations and for ensuring the reliability of the customer/submitted KYCs, in addition to the PAN AMFL will try to verify all the submitted KYC documents online/offline or other services offered by the issuing authorities.

6.2.1. Customer Due Diligence procedure (CDD) in case of individuals

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

- a) A certified copy of Officially Valid Documents (OVD), as given in Annexure I, containing details of proof of their identity and address.
- b) One recent photograph (live photo of the customer will be taken at all possible situations).
- c) In case of MSME, the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- d) Such other documents pertaining to the nature of business or financial status.
- e) In case of Gold Loan, a copy of the PAN Card of the borrower for all transaction above ₹ 5 lakhs.

Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority. The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or the KYC Identifier with an explicit consent to download records from CKYCR;

6.2.2. Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode

AMFL shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. AMFL has a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

6.2.3. Verification of equivalent e-document:

Where the customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer, AMFL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the customer as specified in the guidelines for digital KYC.

6.2.3 Simplified Procedures For Small Value Gold Loans:

For customers with aggregate loans below Rs.0.50 lakh, Proof of Identity alone will be sufficient provided the customer gives full and complete address in the loan application form and his telephone number is confirmed by the branches to be correct. If a person is unable to produce identity documents as mentioned in Annexure I (i.e., any of OVDs), interim / Temporary KYC documents such as Labour card, Civil ID card, Credit Card, Employer Company ID card, LIC card, State ID card, Bank Pass Book, etc. may be accepted subject to the following conditions:

- a) The customer shall provide a self-attested photograph of the customer/ Branches shall take a live photo of the customer.
- b) Branch Head shall certify under his/her signature that the customer has affixed his signature or thumb impression in his presence.
- c) The account shall remain operational initially for 12 months, within which the customer must furnish his identity documents for conducting CDD as mentioned in para 6.2.1. And the customer shall be suitably informed the same at the time of starting the relationship.
- d) Maximum outstanding shall not exceed Rs 0.50 lakh in all their accounts taken

together at any point of time and the total credit in all the accounts taken together shall not exceed Rs.1 lakh in a year.

e) The customer shall be made aware that no further transaction will be permitted until full KYC procedure is completed in case of condition no. d. above is breached.

f) Regularization of Interim/Temporary KYC: In order not to inconvenience the customer, the AMFL shall notify the customer when the balance reaches rupees forty thousand (Rs. 40,000/-) or the total credit in a year reaches rupees eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted and that otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds Rs 0.50 Lakh at any point of time or the total credit in the accounts in year exceeds Rs 1.00 Lakh.

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

6.2.4 Identification of beneficial owner

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

- a. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- b. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

6.2.5 CDD measures in respect of non-individuals:

CDD Standards and documents to be collected in respect of Proprietary firms, partnership firms, companies and other Legal entities are given in Annexure I.

6.2.6 Facilitating third party products

While facilitating third party products, AMFL shall comply with the following directions:

- a. Identity and address of the walk-in customers shall be verified for transactions above Rs 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
- b. Transaction details of facilitation of third-party products and related records shall be maintained as specified under this policy.
- c. AMFL software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be made available.
- d. Transactions involving Rs 0.50 lakh and above shall be undertaken only by:
 - Debit to customer's account or against cheque, transfer from banks / debit cards / credit card etc.
 - In case of MSME loans, obtaining and verifying PAN (regular customer as well as walk in customer).

6.3 RISK MANAGEMENT

AMFL has put in place appropriate procedures to ensure effective implementation of KYC guidelines.

- a. Risk categorization of Customers shall be undertaken based on various factors, 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.
- b. AMFL has categorized its Customers into 'High Risk / Medium Risk / Low Risk' based on the profile of the customers. AMFL shall apply higher due diligence measures keeping in view the risk level. AMFL shall treat the risk categorization and reasons for risk categorization of customers as confidential.
- c. Considering the lower value of transactions and the KYC procedure set aside in the process of microfinance ensures customer risk category as low. Also based on the ongoing monitoring process the status shall get x`.
- d. AMFL has developed robust underwriting procedures for onboarding borrowers for its MSME loan portfolio, which include verification of ownership and the assessment of financial resources of the borrowers, according to the nature and the size of loan offered.
- e. Microfinance customers are lent based on joint liability and collateral free. Income limits are assessed based on their self-declaration. All eligible loans based on the credit bureau verification and the sanction process is automated.
- f. AMFL's internal audit periodically evaluate the level of adherence to the KYC procedures. Audit function shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

6.4. MONITORING OF TRANSACTIONS

- a. AMFL shall monitor transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the AMFL will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose.
- b. AMFL shall exercise caution with respect to the transactions with persons (including legal persons and other financial institutions) from the countries which have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF Recommendations, 2012.
- c. AMFL shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling the terms and the direction of the RBI/PMLA in respect of all products/ services.
Compliance team shall be monitoring and reporting all the necessities.

6.4.1. Ongoing due diligence

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

- b. Any unusual pattern in the operations of the accounts like foreclosure within 6 months, transactions exceeding threshold limits, high turnover in the accounts compared to the average outstanding etc. shall be closely monitored. The extent of monitoring shall be aligned with the risk category of the Customer and high-risk category accounts shall be subjected to more intensified monitoring.
- c. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

6.4.2. Periodic updation

Periodic updation shall be carried out at least once in every two years, for high risk Customers, once in every eight years for medium risk Customers and once in every ten years for low risk Customers from the date of opening of the account / last KYC updation. The procedure for updating the KYC details are as follows;

i. Individual Customers:

- a) No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard will be obtained through customer's registered email-id, registered mobile number, digital channels (mobile application), letter etc.
- b) 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 registered email-id, registered mobile number, digital channels (mobile application), 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.

At the time of periodic Updation, the AMFL will collect any of OVD or the equivalent e-documents thereof mentioned in Annexure 1, in every possible situations.

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. AMFL 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.

ii. Customers other than individuals:

- a) No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its registered email id, digital channels (mobile application), letter from an official authorized by the LE in this regard, board resolution etc. Further, AMFL shall ensure during this process that Beneficial Ownership (BO) information available with AMFL is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- b) Change in KYC information: In case of change in KYC information, AMFL shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

iii. Additional measures

In addition to the above, AMFL shall ensure that –

- a) At the time of periodic Updation, if the existing KYC is not as per the OVD list mentioned in Annexure 1, AMFL will update OVD documents, even if there is no change

in customer information. Further, in case the validity of the CDD documents available with AMFL has expired at the time of periodic updation of KYC, AMFL shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

b) At the time of periodic Updation, customer's PAN details will be verified from the database of the issuing authority.

c) An acknowledgment will be 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.

d) In order to ensure customer convenience, AMFL shall do necessary arrangement to making available the facility of periodic updation of KYC at any branch.

e) AMFL shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures or otherwise adopted by the business verticals will continue as a part of additional monitoring procedures.

f) AMFL shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; AMFL will collect the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at AMFL's end

In addition to the above AMFL shall obtain PAN or Form No.60 by such date notified by the Central Government or at the time of periodic updation whichever is earlier , falling which AMFL shall temporarily cease operations in the account till the time the PAN number of Form No.60 is submitted by the customer.

6.4.3. KYC updation for existing customers

a. In case of existing MSME loan customers, AMFL shall obtain PAN or Form No.60 by such date notified by the Central Government, falling which AMFL shall temporarily cease operations in the account till the time the PAN number of Form No.60 is submitted by the customer.

b. Operations of the MSME loan customers without PAN or Form No.60 shall be monitored closely and shall ensure that transaction does not exceed Rs 5 lakh.

7. A. ENHANCED DUE DILIGENCE

(1) Company shall, prior to the commencement of each specified transaction,—

(a) verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (18 of 2016) in such manner and subject to such conditions, as may be prescribed:

Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhaar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed;

(b) take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed;

- (c) take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
- (2) Where the client fails to fulfill the conditions laid down under sub-section (1), the reporting entity shall not allow the specified transaction to be carried out.
- (3) Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed.
- (4) The information obtained while applying the enhanced due diligence measures under sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

Explanation.—For the purposes of this section, "specified transaction" means—

- (a) any withdrawal or deposit in cash, exceeding such amount;
- (b) any transaction in foreign exchange, exceeding such amount;
- (c) any transaction in any high value imports or remittances;
- (d) such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing,

as may be prescribed.

7.1 Accounts of non-face-to-face customers (other than Aadhaar OTP based

on-boarding): AMFL shall ensure that the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face-to-face customers

7.2 Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

Non-face-to-face onboarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by REs for non face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

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

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

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

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

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

f) Such customers shall be categorized as high-risk customers and accounts

opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP

7.3 Accounts of Politically Exposed Persons (PEP): Special care and diligence will be taken in respect of Politically Exposed Persons. Generally, the AMFL may not (would not) open loan accounts of PEP. However, any request from PEPs shall be escalated to Senior management and will be dealt with based on their approval and will be subject to enhanced due diligence (comprising of additional documents) and monitoring.

- (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 is taken at a senior level in accordance with the AMFL Customer Acceptance Policy.
 - (d) all such accounts are subjected to enhanced monitoring on an on-going basis;
 - (e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship.
 - (f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
- B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

7.3 Client accounts opened by professional intermediaries:

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

- (a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (b) AMFL have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- (c) AMFL will not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to AMFL.
- (d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of , and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of AMFL, the AMFL shall look for the beneficial owners.
- (e) AMFL shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- (f) The ultimate responsibility for knowing the customer lies with the AMFL

B. SIMPLIFIED DUE DILLIGENCE

7.4 Simplified norms for Self Help Groups (SHGs)

- (a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
- (b) CDD of all the office bearers shall suffice.
- (c) Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

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

- (a) Banks shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
 - i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.
 - ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.
- (b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.
- (c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

7.6 Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex III, subject to Income Tax (FATCA/CRS) Rules. Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex III will be submitted

8. CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS

All the information collected from the customers by AMFL shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that behalf.

Information collected from customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Exception to the confidentiality of customer information shall be as under:

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

9. MAINTENANCE OF RECORDS OF TRANSACTIONS

AMFL shall maintain proper records of the transactions as required under the provisions of PML Act and Rules. AMFL shall

- a. maintain all necessary records of transactions between AMFL and the customer, for at least five years from the date of transaction or any other higher periods specified in any other law.
- b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during business relationship, for at least five years after the business relationship is ended or the account has been closed, whichever is later.
- c. 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).
- d. maintain all necessary information in respect of transactions prescribed under PML Rule 3 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.
 - e. AMFL have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

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

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

10. GENERAL

10.1 Adherence to KYC guidelines by agents

AMFL does not engage any agents for carrying out its business and hence this clause is not applicable.

10.2 Principal Officer

AMFL has designated Chief Compliance Officer (CCO) as Principal Officer (PO) responsible for ensuring compliance, monitoring transactions, sharing, and reporting information as required under the law/regulations.

10.3 Designated Director

AMFL has nominated MD, as Designated Director, to ensure overall compliance with the obligations under Prevention of Money laundering Act, 2002 and Rules framed thereunder, from time to time.

10.4 CDD Procedure and sharing KYC information with central KYC records Registry (CKYCR)

AMFL shall capture the KYC information for uploading the data pertaining to all new individual accounts opened on or after 1/4/2017 with the CKYCR in the manner mentioned in the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time. 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.

10.5 Training Program

AMFL shall have adequate screening mechanism as an integral part of personnel recruitment/ hiring process and should have an ongoing employee training programs so that members of the staff are adequately trained in KYC/AML/ Combating the Financing of Terrorism (CFT) procedures. Training requirements shall have different focuses for front line staff and officer/staff dealing with new customers so that all concerned fully understand the rationale behind the KYC policies and implement them

consistently. Such training shall be in house and through external agencies wherever possible.

10.6 Aadhaar Compliance

- a. Where customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, the same shall be masked or blacks out through appropriate means.
- b. The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.
- c. Consent of the Aadhaar number holder shall be collected in situations performing Aadhaar authentication/Offline Verification.

11. COMPLIANCE OF KYC POLICY

- a. AMFL's internal audit and compliance functions periodically evaluate the level of adherence to the KYC policies and procedures. The compliance function and audit function together shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements. The Audit Committee of the Board shall review adherence to the KYC guidelines at quarterly intervals.
- b. Internal Audit shall on a yearly basis conduct an evaluation of compliance functions of policies and procedures including legal and regulatory requirements.
- c. AMFL shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced

Annexure I

CDD & OFFICIALLY VALID DOCUMENTS (OVD)

1. Individuals

Officially Valid Documents (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the voters identity card issued by the election commission of India, job card issued by NREGA duly signed by an Officer of the state government and letter issued by the National Population Register containing details of name and address.

Provided that,

- a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents 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.
- c. the customer shall submit OVD with current address within a period of three months of submitting deemed OVDs

2. Non-Individuals (Companies, Firms, Trusts etc.)

KYC norms are applicable to non-individuals also. The requirements are as under.

<p>Legal entities (Companies)</p>	<p>Certified copies of each of the following documents shall be obtained:</p> <ol style="list-style-type: none"> Certificate of incorporation with Memorandum & Articles of Association Resolution of Board of Directors for opening the account and Power of Attorney / authorization of persons to operate the account on its behalf PAN allotment letter/ PAN of the Company Documents as specified above of the individuals holding attorney /authorisation to transact on company's behalf. CDD of the Individual beneficial owner as specified the names of the relevant persons holding senior management position; and the registered office and the principal place of its business, if it is different.
<p>Partnership Firms</p>	<p>Certified copies of each of the following documents shall be obtained:</p> <ol style="list-style-type: none"> Registration certificate. Partnership deed. PAN of the partnership firm Documents as specified above of the individuals holding attorney /authorisation to transact on its behalf. the names of all the partners and address of the registered office, and the principal place of its business, if it is different
<p>Proprietary firms</p>	<p>For opening an account, CDD of the individual (proprietor) as mentioned shall be carried out PLUS any two of the below mentioned documents,</p> <ol style="list-style-type: none"> Registration certificate including Udyam Registration Certificate (URC) Certificate/License issued under Shops & Establishment Act GST and Income Tax returns GST registration certificate (provisional/ final) Utility bills such as electricity, water, telephone bills etc. 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. IEC (Import Export 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.

<p>Any unincorporated association or a body of individuals</p>	<p>For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> a) Resolution of the managing body of such association or body of individuals b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals c) Power of attorney granted to transact on its behalf d) Documents as specified above, of the person holding an attorney to transact on its behalf and e) Such information as may be required by AMFL to collectively establish the legal existence of such an association or body of individuals.
<p>Trust</p>	<p>Certified copies of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> a) Registration certificate; b) trust deed; and c) Permanent Account Number or Form No.60 of the trust; and d) such documents as are required for an individual under sub-rule (1) 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 and the address of the registered office of the trust; and <p>list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust.</p>

Video based Customer Identification Process (V-CIP)

REs may undertake live V-CIP, to be carried out by an official of the RE, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the RE performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

- Banks: can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP.

ii. RE 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the RE shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the RE shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

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

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

viii. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness, and end to end encryption, the REs shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. REs are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.

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

xiv. BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. Banks shall maintain the details of the BC assisting the customer, where services of BCs are

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

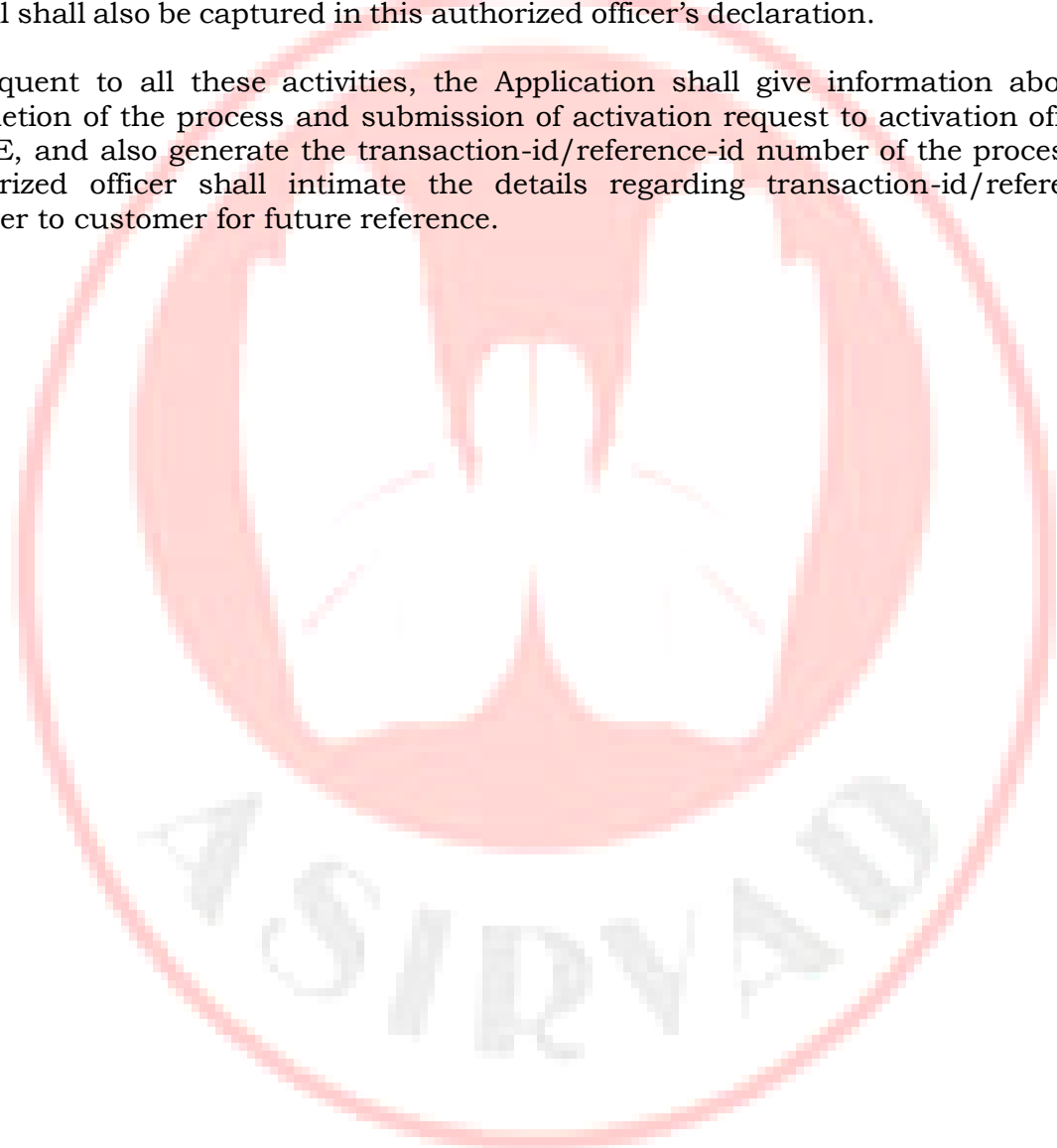
Annexure III

Digital KYC Process (RBI guidelines)

- A. The RE shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the REs.
- B. The access of the Application shall be controlled by the REs, and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by REs to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
- C. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM: YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- D. The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- E. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and watermarking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
- F. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- G. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
- H. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have

his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

- I. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
- J. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.



Annexure-1 Criteria for Risk Classification

Basis	Parameter	Risk Category*	Type of entry**
Identity of the Customer	Customer provided False/Fake/forged KYC Docs (as per audit reports/other sources)	H	S/M
	Other KYC Irregularities (as per audit reports/other sources)	M	S
	KYC verified and found improper (Based on AH Verification Report)	M	S
	No KYC Document	M	S
	No customer photo	M	S
	Wrong customer photo (based on AH verification report)	M	S/M
Social Financial Status	REP/PEP	H	S/M
	Criminal Offences/Adverse Media Reports	H	M
Nature of business/occupation <i>(The existing list to be updated to cover more cases - Annexure-2)</i>	Gold Smith/Jewellers/Jewel worker/Money lenders/ Financiers/Real estate brokers	H	S/M
	Employees - Banks/NBFC/FI	M	S/M
Location of the customer	Customer from other state	M	S
	Loans in more than 2 branches	M	S
	Loans in more than 5 branches	H	S
Address verification	Address does not exist	H	S/M
Multiple Customer IDs	Same customer, Family members, Staff of customer, Group customers	H	S/M
Cash Transactions	Disbursement >Rs.2L in a day or >Rs.9L in a month	M	S
	Disbursement >Rs.4.5L in a day or >Rs.9L in a month (Plus any of the below - No PAN, Not EKYC, No OTP confirmation)	H	S
Inconsistency	Occupation - 'Self Employed' (Auto/Taxi, Driver, Porter, Tea shop, Fisherman, Others) and 'Others' (Politician, Religious leader, Coolie/daily wage worker) having OS > Rs.5L	M	S
	Occupation - 'Self Employed' (Auto/Taxi, Driver, Porter, Tea shop, Fisherman, Others) and 'Others' (Politician, Religious leader, Coolie/daily wage worker) having OS > Rs.10L	H	S
	Others (House wife/Home Service, Student, Unemployed) having OS>Rs.2L	M	S
	Others (House wife/Home Service, Student, Unemployed) having OS>Rs.5L	H	S
Exposure (As on date)	Exposure >Rs.10L	M	S
	Exposure >Rs.10L (Plus any of the below - No PAN, Not EKYC, no OTP confirmation, not registered for OGL/SGL)	H	S
	Exposure >Rs.25L	H	S
Others	Other Parameters	M/H	M

*H=High Risk, M=Medium Risk.

**S=System based, M=Manual, S/M=System and Manual

Annexure – 2 Business/Occupation: The “Business/Occupation” dropdown list to be modified as below:

Sl. No.	Category 1	Sub Category 1	Sub Category 2
1	Agriculture		
2	Salaried	Public Ltd Private Ltd MNC Educational Inst Central/State Govt. Public Sector Unit Proprietorship Partnership Banks NBFC Financial Institutions Others	
3	Business	Trader	Home Appliances Medical shop Provisions store Stationery Textiles Others
		Whole-seller	Home Appliances Medical shop Provisions Stationery Textiles Others
		Manufacturer	Home Appliances Medicines Stationery Textiles Others
		Others	Hotel/Bakery Construction Real estate Transport Others
4	Jewellers	Retailer Whole-seller Manufacturer	
5	Gold Smith/Jewel worker		
6	Professional	Doctor CA/CWA/CS or Equivalent Architect Lawyer Actors/Celebrities Others	

7	Self Employed	Auto/Taxi Tailoring unit Workshop Driver Porter Tea shop Fisherman Others	
8	Money Lenders/Financiers	Pawn broker Others	
9	Others	House wife/Home Service Student NRI Pensioner/Retired Politician Religious leader Media/Press Coolie/daily wage worker Unemployed	

