Know Your Customer Norms and Anti-Money Laundering Policy

of

Finagle Financial Services Private Limited

on

May 23, 2026

_____

Rupali Mathur
Director

Document Information

Name:	Know Your Customer Norms and Anti-Money Laundering Policy
Area:	Legal and Compliance
Key concepts:	KYC, AML, CFT, Risk Management, Customer Identification and Due Diligence, Periodic Updation, Monitoring and Reporting, Record Management, Training
Responsible Department/Function:	Compliance
Department Version No.:	7
Effective Date:	May 23, 2026

Version Number	Reason for change	Author
Version 7	Annual Review	Compliance Department

Table of Content Page

1 Objective and Scope

1.1 Objective

The objective of this policy framework is to:

a) provide sufficient framework for placing and implementing adequate systems and procedures for customer acceptance, customer identification, monitoring the transactions of the customers and taking measures for mitigating the risk of Money Laundering and Terrorist Financing.

b) put in place systems and procedures to help identify money laundering and suspicious activities and safeguarding the Company from being unwittingly used for the transfer or deposit of funds derived from criminal activity or for financing of terrorism.

1.2 Scope

RBI has issued relevant directions on Know Your Customer (KYC) time to time in the context of the Recommendations made by the FATF on AML standards. Financial Intelligence Unit -India has also issued guidance for NBFCs on effective processes for detecting and reporting suspicious transactions. The Company shall, therefore, adopt the same with suitable modifications depending upon the activity undertaken by the Company and ensure that a proper policy framework on KYC and AML measures is formulated and put in place with the approval of the Board of Directors of the Company.

The provisions contained in this Policy in respect of KYC Compliance and procedures shall apply to the Company except in so far as the same are inconsistent with any statutory modification thereof, including any applicable judicial pronouncement(s). In case of any contradiction, the statutory modified provisions and/or the applicable judicial pronouncement shall prevail.

1.3 Regulatory Context

The Policy takes into account regulatory documents published by regulatory bodies, as and when become applicable (hereinafter collectively referred as "Applicable Laws"), in particular:

- Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, as amended from time to time till the date of this Policy (hereinafter referred as "KYC Norms")
- Prevention of Money Laundering Act and the rules/ regulations issued thereunder as applicable to the Company as amended from time to time till the date of this Policy (hereinafter referred as "PMLA")
- Guidance Note issued by FIU-IND till date on Effective Processes of STRs Detection and Reporting for Non-Banking Financial Companies (hereinafter referred as "Guidance Note")

1.4 Related Documents

The Policy represents an integral part of the overall risk management of the Company. Further, the process documents/ standard operating procedures on following matters shall form part of the Policy:

a. Customer Risk Categorisation Model
b. Sanction Screening and Transaction Monitoring
c. Video-KYC
d. Reporting to CKYCR

1.5 Definitions and Abbreviations

The meaning of capitalised terms and abbreviations used in this Policy is set out below. The words and abbreviations used in this Policy shall have the same meaning as defined in KYC Norms issued by RBI, as amended from time unless the same has been defined explicitly in this Policy.

"Audit Committee" means the committee of directors constituted, or to be constituted, by the Board to discharge the roles & responsibilities specified under the provisions of Section 177 of the Companies Act, 2013 read with para 3 of Corporate Governance (Reserve Bank) Directions, 2015 issued by Reserve Bank of India;

"AML" means Anti-Money Laundering;

"Board" means the Board of Directors of the Company constituted under the provisions of the Companies Act, 2013;

"Beneficial Ownership/Owner" means the natural person(s), who, whether acting alone or together or through one or more juridical persons, has/have -

a) In case of a Company, controlling ownership interest or who exercises control through other means, where-
"Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company, and
"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) In case of a partnership firm, ownership of/entitlement to more than 10 per cent of capital or profits of the partnership. "Control" shall include the right to control the management or policy decision.
c) In case of an unincorporated association or body of individuals, 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.
d) In case of a trust, the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Cash Transactions" mean and include:

a) all cash transactions of the value of more than Rs.10,00,000/- (Ten Lakh Rupees only) or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10,00,000/- (Ten Lakh Rupees only) or its equivalent in foreign currency where such series of transactions have taken place within a month, and the aggregate value of such transactions exceeds Rs.10,00,000/- (Ten Lakh Rupees only) or its equivalent in foreign currency; and

c) 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 or document has taken place.

"CEO" means the Chief Executive Officer of the

Company; **"CFT"** means Combating of Financing of

Terrorism; **"Customer"** may be defined as:

(a) A person or entity who is engaged in a financial transaction or activity with the Company.

(b) A person on whose behalf the person who is engaged in the transaction or activity, is acting (i.e. the beneficial owner).

"Customer Identification" means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

"CERSAI" means Central Registry of Securitisation Asset Reconstruction and Security Interest of India;

"CKYCR" means Central KYC Registry set up by the Government of India to receive, store, safeguard and retrieve the KYC records in the digital form of a client and to act as a centralized repository of KYC records of customers in the financial sector and inter-usability of the KYC records across the sector;

"Compliance Department" means the Compliance Department of the Company;

"Digital Lending Platforms/ Channels" means loans disbursed through digital lending platforms/ channels imply loans taken through signing on digital lending app/ web platform, whether or not assisted by the Company representative;

"FATF" means Financial Action Task Force;

"FIU-IND" means Financial Intelligence Unit – India;

"High Net Worth" means a net worth of INR 50 million or more;

"Identity" generally means a set of attributes which together uniquely identify a natural or legal person. Following attributes, combination thereof, should be considered for satisfying with the identity of the individual Customer.

a) Name,
b) Photograph,
c) Date of Birth,
d) Father's/ Mother's/ Spouse's name,
e) Residential address

"KYC" means Know Your Customer;

"NBFC" means Non-Banking Financial Company;

"NSDL" means National Securities Depository Limited;

"Offence of Money Laundering" is defined as: "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering." Money Laundering is moving illegally acquired money through financial systems so that it appears to be legally acquired. There are three common stages of money laundering - (a) Placement – the physical disposal of cash proceeds derived from illegal activity. (b) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and create anonymity; and (c) Integration – creating the impression of apparent legitimacy to criminally derived wealth;

"Officer at the Management Level", for the purpose of this Policy, means and includes the the employee of the Company upto two levels below Chief Executive Officer of the Company (CEO-2).

"PEP" or "**Politically Exposed Persons**" means individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. and declares such status to the Company while availing loan from the Company;

"RBI" means Reserve Bank of India;

"Residential Address" means the address at which a person usually resides and can be taken as the address as mentioned in documents accepted by the Company for verification of the address of the Customer.

"Senior Management" , for the purpose of this Policy, means and includes Chief Executive Officer and the function heads of the Company;

a) **"Screening List"** means the list, maintained by the Company for screening of the Customers and shall include lists prescribed by RBI, FIU-IND or any other concerned authorities time to time or the list internally maintained by the Company basis which the Company shall identify Unacceptable High Risk customers as per this Policy and take appropriate action.

"STR" means Suspicious Transaction Report;

"Sanctions" or "Sanction List" means the lists of individuals and entities that any one or more of E.U., U.S., U.N. or Interpol, Economic Offence Wing and/ or Ministry of Home Affairs, as available to the Company from time to time, or any other local authority, including RBI, has listed as the target or subject of Sanctions, including checks based on specific geographies, government and restricted activities (prescribed by Company). The updated list of terrorist organisations, namely, ISIL (Da'esh) & Al-Qaida Sanctions List and 1988 Sanctions List can be accessed at the United Nations website;

"Suspicious transaction" means a transaction, including an attempted transaction whether or not made in cash, which, to a person acting in good faith-
(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to have no economic rationale or bonafide purpose; or
(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
Explanation - Transaction involving financing of activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

"Terrorist financing" is, in general, the processing of legally or illegally sourced funds or other financial assets to sponsor or facilitate terrorist activity (hereinafter the "Terrorist Financing/ TF/ CTF");

"UCIC" means Unique Customer Identification Code; and

"UIDAI" means Unique Identification Authority of India.

Unless defined herein, all other expressions shall have the same meaning as has been assigned to them under the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

2 Roles and Responsibilities

2.1 Board of Directors

2.1.1 The Board of Directors of the NBFC, or any committee to which the Board has delegated power, shall duly approve the KYC Policy

2.1.2 The Board shall appoint a Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.

2.1.3 The Board shall appoint an officer at the management level as Principal Officer.

2.1.4 The Board, or the Committe thereof, shall review the outcome of the 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercises carried out by the Company

2.1.5 The Board, or the Committee thereof, shall determine the periodicity of the risk assessment exercise, not lesser than annual, in alignment with the outcome of the risk assessment exercise.

2.1.6 The Board shall ensure that the decision-making functions of determining compliance with KYC norms shall not be outsourced.

2.2 Designated Director

The Board shall appoint a "Designated Director" to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The name, designation, contact details and address of the Designated Director shall be communicated to the Reserve Bank of India and FIU-IND. In no case, the Principal Officer shall be nominated as the 'Designated Director'.

In accordance with the specific terms and conditions applicable to the Company, as outlined by the RBI in its letter dated July 10, 2018, regarding grant of registration as NBFC, the Company shall within one month of starting its commercial business, communicate the name, designation and address of the Principal Officer and Designated Director to the Financial Intelligence Unit-India (FIU-IND) and shall intimate the same to the Regional Office of RBI under whose jurisdiction the registered office of the Company is located, not later than one month of such appointment. The "Designated Director" means a person designated by the company to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. NBFCs can also designate a person who holds the position of senior management or equivalent as "Designated Director".

2.3 Principal Officer

The Board shall appoint an senior officer at the management level as Principal Officer. The name, designation, address and contact details of the Principal Officer shall be communicated to the Reserve Bank of India and FIU-IND. Principal Officer shall be responsible for –

2.3.1 ensuring compliance, monitoring of all transactions and reporting information to the regulatory authorities as required under the applicable law/ regulations.

2.3.2 maintaining close liaison with regulatory bodies and enforcement agencies.

2.3.3 overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Act and Rules, as amended from time to time.

2.3.4 the Principal Officer and other appropriate staff should have timely access to customer identification data and other customer due diligence information, transaction records and other relevant information.

2.3.5 must act independently and report compliances under this Policy to the Board.

2.4 Internal Audit

2.4.1 The Company should have effective and efficient internal audit to evaluate and ensure adherence to the KYC policies and procedures. The internal audit should oversee the activities conducted by Company's business front line and compliance function and provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

2.4.2 Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard in the form of quarterly audit notes shall be placed before the Board, or the Audit Committee, as the case may be.

2.5 Other roles with respect to ensuring adherence to KYC Policy and Procedures

2.5.1 The Senior Management shall be responsible for ensuring compliance with the KYC Policy and Procedures.

2.5.2 The Company business front line/ departments and the head of business of front line/ departments shall be responsible and accountable for ensuring compliance with AML/ CTF laws and this Policy within their respective departments, and deployment of requisite controls and day-to-day management of associated risks, including those associated with contractual arrangements which bind the Company.

2.5.3 The Compliance Department shall ensure that requisite policies and procedural documents are approved and implemented expressly stating the allocation of responsibility of respective departments of the Company for effective implementation of such policies and procedures.

2.5.4 The CEO of the Company shall ensure adequate resources to enable carrying-out respective responsibilities under this Policy.

2.5.5 HR Department shall ensure background verification of all employees of the Company and appropriate training to the employee on the Policy and Applicable Law.

2.5.6 Anti-Fraud Department shall assist Principal Officer in Sanction Screening and

.Confidentiality and sharing of customer Information

The Company shall maintain the confidentiality of customer information which arises out of the contractual relationship between the Company and the customer. While preparing customer profiles, the Company should take care to seek only such information from the customer which is not intrusive and maintain secrecy of such information. While considering the requests for data/ information from the Government and other agencies, the Company shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

The Company shall maintain the confidentiality of customer information:

a) collected from customers for the purpose of opening of account. Such details shall not be divulged for the purpose of cross-selling or for any other purpose without the express permission of the customer.

b) contained in any statement or return submitted by such company under the Reserve Bank of India Act, 1932; or

c) obtained through audit or inspection or otherwise by the RBI, except in the following cases:

   i. information disclosed with the previous permission of RBI;

   ii. information published by RBI, if it considers necessary in public interest to do so, without disclosing the name of the NBFC or its borrowers; or

   iii. where disclosure is in accordance with the practice and usage customary amongst such companies or as permitted or required under any other law for the time being force

The exceptions to this provision are -

a) Where disclosure is under compulsion of law;

b) Where there is a duty to the public to disclose;

c) Where the interest of the company requires disclosure, or

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

3 Customer Acceptance Policy

The Company should develop & implement a clear process for acceptance of a person or entity as a 'Customer'. The Company shall ensure that:

3.1 Avoid anonymous, fictitious or benami customers.

The Company must ensure that no loan shall be provided in, or business relationship shall be entered with, anonymous or fictitious/ benami name(s). The processes of the Company must ensure that such transactions are rejected at the application stage only.

3.2 Avoid customers with criminal background.

The Company shall maintain a Screening List of persons as available in public domain and/ or accessible to the Company. The Company should ensure duplication check during the

stage of acceptance of the customer and/ or during regular reviews of the portfolio, including of relationships which may involve accepting assets that are known or suspected to be proceeds of criminal activities or to be used for or in connection with terrorist activities.

3.3 Avoid customers to whom KYC procedures cannot be applied.

The Company shall not grant a loan to any person who fails to abide by the extant KYC Norms prescribed by RBI. Before granting loans or entering into any business relationship, the Company must ensure that the customer is verified and identified and the data/ information furnished to the
Company is reliable. However, the Company should ensure that no harassment shall be caused to the customer.

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company should close the loan account or terminate the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. The Company should prescribe a detailed process to identify such cases, verifying if the customer has a genuine issue in non-complying with KYC measures of the Company or if the customer is involved in any fraudulent, money laundering, financing of terrorist activities, obtaining requisite information required for decision-making purposes and closing the account of the customer if so decided.

The Company shall consider filing a Suspicious Transaction Report (STR), if necessary, where the Company forms a suspicion of money laundering or terrorist financing, or it is unable to comply with the relevant customer due diligence measures in relation to the customer or where the Company reasonably believes that performing the due diligence process will tip-off the customer.

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

3.4 Avoid sanction of loans applied through intermediaries.

The Company shall put in place adequate systems, processes and controls to ensure that no loan is sanctioned/ approved if applied by/ through an intermediary or on behalf of another person/ entity.

3.5 Avoid grant of loans to the joint-borrowers

The Company shall put in place adequate systems, processes and controls to ensure that no loan is sanctioned/ approved if applied by two or more borrowers jointly.

3.6 Adequate information to customers on customer due diligence procedure.

The Company shall inform the customers in advance about the mandatory information required for KYC purposes along with loan application as well as during the periodic updation. Where the Company needs additional information, such information should be obtained with the explicit consent of the customer. The Company shall apply the customer due diligence

procedure at the UCIC level. The Company shall ensure that introduction is not to be sought while opening loan accounts.

3.7 Verification of Customer's Documents

Permanent Account Number (PAN) obtained from the customer shall be verified from the verification facility of the issuing authority or an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000

3.8 Financial Facility to financially or socially disadvantaged, including the Persons with Disabilities (PwDs)

The Company shall not deny any financial facility to persons who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs) solely on the ground of such disadvantage. The Company shall not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned shall duly record the reason(s) for rejection.

3.9 Operation of accounts and Money Mules

The Company shall ensure that no account is opened for money mules and the instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to accounts by recruiting third parties which act as "money mules." The Company shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as money mules and take appropriate action, including reporting of suspicious transactions to FIU-IND.

4 Risk Management

4.1 Anti – Money Laundering Risk Categorisation of Customers

For the purpose of complying with the Policy, the customers should be categorised into low, medium, high and unacceptable high risk based upon the risk parameters for which adequate information/ data must be collected at the application stage i.e. type of loan product offered, purpose of availing loan, customer's identity, location of customer, source of funds to estimate the social/financial status, nature of business activity, customer's past/ existing relationship with the Company and delivery channel used for application/ grant of loan.

However, while preparing a customer profile, the Company should take care to specify and seek only such information from the customer which is either relevant to the risk category or required by law and is not intrusive. The documents and/ or information should be collected from the customer keeping in mind the perceived risk associated with such customer and regulatory requirements applicable from time to time. Based on the information/ data provided by the customer and due verification of such information/ data the decision shall be taken accordingly on the loan application of such customer. Least manual intervention

should be ensured in such decision-making process and the help of information technology should be taken to the extent possible. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Based on the aforesaid risk parameters, the customers shall be categorised into below stated risk categories (refer **Annexure 1** for detail):

a) Unacceptable High Risk Customers
b) Acceptable High Risk Customers
c) Medium Risk Customers
d) Low Risk Customers

The risk rating model of the Company shall be based on the weighted risk computation wherein each parameter is assigned a 'risk score' and a 'weight' is attached to the parameter depending upon its criticality to the overall risk. The output score is compared to a final scale. While assigning risk score and weight to various parameters, critical and more accurate parameters shall be given their due weightage from AML risk perspective for the purpose of risk scoring the customer. The Company may, from time to time revisit the weights and parameters based on regulations, market behaviour and industry practices.

The Company shall keep the risk categorisation of a customer and the specific reasons for such categorisation confidential and shall not reveal this information to the customer to avoid tipping off.

4.2 Customer Screening

a) Customer Screening constitutes a crucial step in the risk assessment process requiring screening of the name/s of the Customers against the Screening List. The Company should ensure that all applications of the Customers are screened against the internal De-dupe database/ Screening List before the Customer account is opened.
b) The Company shall have requisite mechanism for screening the customers at the application stage, wherein various data collected from the customer shall be analyzed basis pre-defined parameters and checks in the decision-making system, to evaluate the repayment capacity of the customer as well as for prevention of fraud/ money laundering activity against the Company.
c) The Screening List and internal de-dupe database shall be updated from time to time, including as and when updated by the RBI or concerned authority.
d) In the event Customer's name appears on the Screening List, depending on the list, either the Customer risk rating/ categorisation may be revised and requisite customer due diligence or enhanced due diligence measures be applied wherever required, or the Customer's data shall be reported to the concerned authority, as the case may be.
e) The Screening List/de-dup engine used for screening through the Screening List shall provide a report on the results of screening and be available with the customer loan application documents.

5 Customer Identification Procedures

The Company should obtain sufficient information necessary to establish, to their satisfaction, the identity of each new Customer and the purpose of the intended nature of the relationship. Any additional information about the Customer, if needed, shall be obtained with the consent of the Customer.

5.1 Cases When Customer Needs To Be Identified

The Company must set up adequate procedures to identify customers in the following cases (as applicable) in the normal course of transaction with the customer:

a) Commencement of an account-based relationship with the customer.
b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c) Selling third party products.
d) When there is a reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

The Company shall ensure that introduction is not to be sought while opening accounts.

5.2 Allotment of Unique Customer Identification Code ("UCIC") to customers

In order to avoid multiple identities within the Company, the Company shall allot a unique identification code for each customer while entering into new relationships with individual customers as also the existing individual customers., UCIC will help the Company to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Company to have a better approach to risk profiling of customers. Thus, if an existing KYC-compliant customer of the Company desires to open another account or avail of any other product or service from the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

6 Customer Due Diligence Measures

6.1 CDD Procedure

The Company shall apply the following procedures while establishing any relationship with any customer.

6.1.1 CDD Procedure in case of Individuals

The Company shall apply the following procedure while establishing any relationship with an individual Customer:

a) Obtain information/ document as per **Annexure 2** for verification of identity and address of the individual Customer.
b) Obtain one recent photograph of the individual Customer

c) Obtain such other documents including in respect of the nature of business, financial status of the client etc. as may be required by other policies of the Company

6.1.2 CDD Procedure in case of Medium Risk Customers

The Company shall include following procedure for enhanced due diligence of Medium Risk customers:

a) The identity and address of the Customer applying for the loan shall be verified by following the CDD process as prescribed in Para 6.1.1;
b) The Customer must opt for the repayment of loan instalments only through the normal banking channel (i.e. NEFT/IMPS/ ECS/ ACH/ DD/ UPI etc.) and no cash shall be accepted from such customers.

6.1.3 CDD Procedure in case of Acceptable High Risk Customers

The Company shall include the following procedure for enhanced due diligence of Acceptable High Risk customers:

a) The identity and address of the Customer applying for the loan shall be verified by following the CDD process as prescribed in Para 6.1.2;
b) The primary mobile number of the customer should not be changed without robust verification process and all transactions pursuant to the loan account i.e. transaction OTP, transaction updates, etc., shall be linked only to the primary mobile number.
c) The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
d) The Customer's KYC complied bank account with another Regulated Entity to be verified.

Basis the loan amount and tenure opted by the customer, the Company may provide V-CIP as the first option to the customer for remote onboarding. Further, the customers onboarded in non-face to face mode shall be categorized as high-risk customers until the identity of the customer is verified in face-to-face manner or through V-CIP.

6.1.4 CDD Procedure in case of non-individual customers

The Company grants loans only to individuals. However, the Company has financial relationship with entities as well viz. companies, partnership firms, proprietorship firms, or any other entity. For entering into any such relationship, certified copies of the following documents or equivalent e-dcouments shall be obtained:

a) Charter documents of the entity;
b) Certificate of registration issued by any regulatory authority/ similar information available in the public domain or authority website.
c) Permanent Account Number of the entity
d) A resolution from the Board of Directors/ power of attorney/ letter of authority granted to its authorised employees to transact on its behalf.
e) List of directors/ partners, shareholders and/ or beneficial owners

Further, the CDD procedure, as applicable in the case of individual Customers shall mutatis mutandis apply to the authorised employees of the entity as per Annexure 2.

In case of entities, the Beneficial Ownership of such entity needs to be determined. Provided that:

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

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

Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.

6.2 Identification and Verification process

The Company may have in place one or more of the processes to identify and verify the customers at the time of applying for a loan as enlisted below. Appropriate methods of verification of customer identity be adopted given the nature of the business process, the products and services provided and the associated risks.

a) Digital KYC:
This process entails in-person submission of a copy of an OVD as proof of identity and address by the customer while submitting the loan application, duly verified and confirmed by way of a declaration by the authorised official of the Company. The Company shall follow the process as prescribed by RBI to perform a seamless, secure and real-time interaction with the customer to perform customer verification.

b) Verification through the online database of the Government of India:
This process entails the use of an online database of individuals made available by the Government of India (e.g.. offline method (.xml utility provided by UIDAI) of Aadhaar verification, documents issued by various Government Departments and available in Digilocker. CKYC, NSDL etc.) for identification and verification of customers. These methods should allow the Company to obtain customer information on real-time basis. The Company shall ensure that up to date information, available in authentic database is used for customer verification. PAN submitted by the customer can also be verified through NSDL online facility. The said information is also recorded in all the loan documents submitted by the customer.

c) Due diligence of Existing Customer:

The Company has assigned the UCIC to each of its customers. Based on matching of the customer information against the pre-available personal information at the time of loan application, wherever a change in the customer data is identified, the customer due diligence process shall be carried out.

d) Verification through Third Party

For the purpose of verifying the identity of customers, the Company may rely on customer due diligence done by a third party in compliance with the KYC Norms issued by RBI from time to time, including but not limited to the following conditions for verifying the identity of customers:

i. Records or the information of the customer due diligence carried out by the third party is obtained within the regulatory prescribed period from the third party or from CKYCR.
ii. Adequate steps are taken by the Company to satisfy that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
iii. The third party is regulated, supervised or monitored by RBI or any other regulator, and has measures in place for compliance with customer due diligence and record-keeping requirements under the provisions of PMLA
iv. The third party shall not be based in a country or jurisdiction assessed as high risk.
v. The agreement with such third party should explicitly cover appropriate provisions covering the aforesaid conditions for verifying the identity of customers.

The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company and shall never be outsourced. In this regard, the Company need to ensure that any deviations, if any, in the customer KYC is validated and verified as per applicable laws from time to time.

e) Verification through the Central KYC Records Registry (CKYCR)

Subject to the consent of the Customer, the Company may verify the customer identity and address through the data fetched from CKYCR. Further, the customer should have the option to submit KYC Identifier (i.e. a unique number or code assigned to customer by the Central KYC Records Registry) to the Company for enabling the Company to retrieve the customer identity and address information and records digitally from the CKYCR. The Company may seek information/ documents from the customer if-

i. There is a change in the information of the customer as existing in the records of CKYCR;
ii. The address of the customer is required to be verified;
iii. 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 customer.

f) Video-Based Customer Identification Process ("V-CIP")

For the purpose of verifying the identity of customers, the Company may undertake live V-CIP with an individual customer, after obtaining his informed consent. The Company shall follow the process as prescribed by RBI to perform a seamless, secure, real-time, consent-based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purposes, and to ascertain the veracity of the information furnished by the customer. Such a process shall be treated as a face-to-face process of customer identification.

It is hereby clarified that the Customers onboarded through the digital lending platform and the identity of such Customers verified through any of the following due diligence processes shall be considered as 'non face to face customers' categorised under 'Acceptable High Risk Customers' until the identity of the customer is verified in face-to-face manner or through V-CIP –

- Verification through online database of Government of India
- Verification through Third Party
- Verification through the Central KYC Records Registry (CKYCR)

7 Periodic Updation of Records of the Customer

7.1 The Company should have a risk based approach/ system of periodical updation of identification data (including photograph/s) of existing customers (i.e. excluding the customers who are paid off/ written off) after the loan application is approved. The periodicity of such updation shall be as under:

a) Acceptable High Risk Customers - Once in every two (2) years from the date of submission of the KYC at the time of onboarding with the Company, or last KYC updation, whichever is later.

b) Medium Risk Customers - Once in every eight (8) years from the date of submission of the KYC at the time of onboarding with Company or last KYC updation, whichever is later

c) Low Risk Customers - Once in every ten (10) years from the date of submission of the KYC at the time of onboarding with Company or last KYC updation, whichever is later

In case there is no change in the customer information but the documents available with the Company are not as per the customer due diligence requirement as prescribed under this Policy, periodic updation shall be carried out by the Company equivalent to that applicable for on-boarding a new customer.

Further, in case the validity of the documents available with the Company has expired at the time of periodic updation, or application received for subsequent loan from the Customer, as the case may be, the periodic updation to be carried out by the Company shall be equivalent to due diligence followed for on-boarding a new customer.

NSDL verification of PAN details to be done for the concerned customer eligible of Re-KYC at the time of periodic updation.

The Company shall ensure that the enhanced due diligence measures in respect of Acceptable High Risk Customers as prescribed under this Policy are adhered to.

The Company shall ensure to provide acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation with the date of having performed the updation.

Before granting another loan to the existing Customer, the Company shall seek the necessary information from the Customer to check if there is any change in information provided by the customer earlier. Such verification may happen even if the period of two/ eight/ ten years has not elapsed since the date of the first loan, or last verification, as the case may be.

The Company shall advise the customers that in order to comply with the Applicable Laws, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents within 30 days of the update to the documents for the purpose of updating the records at the Company's end. The Company shall provide adequate facility to the customers for such purpose

7.2 Due Notices for Periodic Updation of KYC:

The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options / channels for complying with the requirement of periodic updation of KYC.

Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations.

The letter of intimation / reminder may, inter alia, contain easy-to-understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation / reminder shall be duly recorded in the Company's system against each customer for audit trail.

7.3 Updation of residential address by the Customer:

The customer may request the update of the residential address by providing to the Company his/ her Aadhaar in electronic form digitally signed by the concerned authority in such manner as specified by the Company in compliance with Applicable Laws.

7.4 Updation of the registered mobile number by the Customer:

The Company shall have suitable process to change the registered mobile number of the customer in its records after due verification. In order to prevent frauds, alternate mobile numbers

shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. The Company shall permit transactions only from the mobile number used for account opening.

The customer may request the update of the residential address by providing to the Company his/ her Aadhaar in electronic form digitally signed by the concerned authority in such manner as specified by the Company in compliance with Applicable Laws.

8 On-going Due Diligence and Monitoring of Transactions

8.1 Ongoing Due Diligence

The Company shall undertake on-going due diligence of customers to ensure that the transactions with such customers are consistent with their knowledge about the customers, customers' business, risk profile and the source of funds. For ongoing due diligence, the Company shall implement appropriate AML software and other suitable tools/ technologies to support effective monitoring.

The extent of monitoring shall be aligned with the risk category of the customer. 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, if required, shall be put in place.

8.2 Monitoring of Transactions

The Company shall ensure regular monitoring of the transactions of the customer with the Company. Such monitoring should cover:

- Mode of repayment of loan by the customer;
- Early repayment by customer;
- Subsequent loan application made by the same customer
- Requests/ complaints raised by the customer
- Large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

a) Repayment by third party not relative of the Customer.

- High account of repayments inconsistent with the income declared by the customer.

b) Transactions which exceed the thresholds prescribed for specific categories of accounts

With a view to ensuring that amounts are paid out of clearly identifiable sources of funds, the Company shall ensure that no cash of Rs.50,000/- and above is accepted from a Customer/ any other intermediary (auction cases) without obtaining a copy of the PAN card/ Form 60 of the Customer/any other intermediary along with a valid identity proof and signature proof, should be accepted.

The extent of monitoring should depend on the risk sensitivity of the customer and should not result in undue harassment to the bona fide customers.

8.3 Commercial Judgment

The Company shall usually adopt the risk-based approach to the KYC requirements. Consequently, there can be circumstances when it will be both necessary and permissible to apply commercial judgment while verifying the customer. The decision on the admissibility of the customer shall be taken on the result of verification, social/ financial status of the customer apart from the documents submitted by the customer.

Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents/office records/ memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Officer for recording his/her findings.

8.4 Alert generation and management

The Company shall have effective monitoring procedures including systems to generate alerts in case of any suspicious transactions or violation of the Policy. The Company shall adopt a process defining roles and responsibilities of various functions/ departments in relation to monitoring of transactions and alert management requirements, including:

a) The Company shall put in place an appropriate software application / mechanism to throw alerts for the transactions that are suspicious considering the profile of customers. The Company shall adopt a process of creation/ generation of alerts whereby certain transactions are flagged on the basis of a set of pre-determined rules or scenarios by which it monitors any transaction which may be unusual, and which may (or may not) be for money laundering/ terrorist financing.

b) For the purpose of generation of alerts, the Company may adopt certain threshold limits, ensure confidentiality and should not circulate /share with other teams within the organisation (other than for the purpose of implementation or automation of the alert generation process), to avoid tipping off.

c) The alerts may be generated through various sources, viz. Customer verification, law enforcement agency query, adverse media reports, employee initiated/ whistle blower, public complaint or information received from business associates like service providers, agents, etc.

d) The Company shall review the alerts generated through various sources based on pre-defined criteria to assess whether a particular customer poses a higher risk of money laundering before submission as STR. The Company shall have an internal process of highlighting and acting on questionable transactions. The Company shall have a detailed process of review of alerts including factors considered for the review, probable grounds of suspicion, etc.

e) The system should maintain a history of all previously generated alerts that were investigated and earlier alerts should also be available during the review process.

f) Cases declared as suspicious post PO review shall be reported as STR (refer section - Reporting of Transactions) as per timelines and format prescribed under the applicable regulations.

g) Company should provide proper communication channel to the employees for reporting, viz. common email ID for reporting alerts, online filing of alert, etc.

The Company shall ensure independent audit of the entire process of alert generation, monitoring and reporting of transaction is reviewed by internal auditors on a yearly basis (at least) to ensure that the process of monitoring and reporting is effective and follow up of actionables, if any, be adhered to within agreed timelines.

8.5 Money Laundering and Terrorist Financing Risk Assessment

The Company shall carry out 'Money Laundering and Terrorist Financing Risk Assessment' exercise at least annually to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The Company shall formulate and design a risk assessment process taking into consideration:

a) all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

b) the overall sector-specific vulnerabilities, if any, that the RBI may share with the Company from time to time;

c) the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

The Company shall apply a risk-based approach for mitigation and management of the risks (identified on their own or through national risk assessment) during such assessment and prescribe appropriate controls and procedures in this regard and monitor the implementation of such controls and enhance them, if necessary.

The Company shall properly document its risk assessment and it shall be proportionate to the nature, size, geographical presence, complexity of activities / structure, etc. of the Company. The outcome of such assessment shall be approved by the Board or any committee of the Board to which power in this regard has been delegated. The outcome shall also be made available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on its own or through national risk assessment) and shall have Board-approved policies, controls and procedures in this regard. The Company shall implement a CDD programme, having regard to the ML / TF risks identified and the size of business. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

9 Confidentiality and sharing of customer Information

The Company shall maintain the confidentiality of customer information which arises out of the contractual relationship between the Company and the customer. While preparing customer profiles, the Company should take care to seek only such information from the customer which is not intrusive and maintain secrecy of such information. While considering the requests for data/ information from the Government and other agencies, the Company shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

The Company shall maintain the confidentiality of customer information:

a) collected from customers for the purpose of opening of account. Such details shall not be divulged for the purpose of cross-selling or for any other purpose without the express permission of the customer.

b) contained in any statement or return submitted by such company under the Reserve Bank of India Act, 1932; or

c) obtained through audit or inspection or otherwise by the RBI, except in the following cases:

i. information disclosed with the previous permission of RBI;

ii. information published by RBI, if it considers necessary in public interest to do so, without disclosing the name of the NBFC or its borrowers; or

iii. where disclosure is in accordance with the practice and usage customary amongst such companies or as permitted or required under any other law for the time being force

The exceptions to this provision are -

a) Where disclosure is under compulsion of law;

b) Where there is a duty to the public to disclose;

c) Where the interest of the company requires disclosure, or

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

10 Record Management

10.1 Preservation and maintenance of records of Customer's identity and transactions

The Company shall maintain all necessary records of transactions including the documents/ proofs of identity and address of the customer and analysis of records in the following manner:

Sr. No.	Nature of Document/ Information
1.	Identity proof of customer (where the identity of the Customer is verified using online facility/ database, necessary evidence of such verification shall be preserved)
2.	Address proof of customer (where the address of the Customer is verified using online facility/ database, necessary evidence of such verification shall be preserved)

3.	Photograph of customer
4.	Loan documents of customer (eg. Loan agreement, application, key fact statement, sanction letter etc)
5.	Transaction document of customers (repayment receipts, ECS/ DD mandates)
6.	Complaints/ Requests of customer, including through mobile application, e-mails and calls
7.	Logs of the transactions performed, approvals and consents given by the Customer in online/ electronic mode
8.	All cash transactions or series of cash transactions above prescribed thresholds and all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002
9.	In respect of the transactions referred above, the Company shall maintain record of the following information also: a) the nature of the transactions; b) the amount of the transaction and the currency in which it was denominated; c) the date on which the transaction was conducted; and d) the parties to the transaction.

10.2 Preservation Period

a) Maintain record of transactions for at least 05 years from the date of the transaction;
b) Maintain records of identification and addresses of customers while opening the account and during the period of business relationship with customer and at least 05 years after the cessation of relationship.

10.3 Preservation Method

a) The data/ information as available in hard copy or soft copy (in some electronic system/ device) shall be preserved in hard copy or soft copy, respectively, during the period of relationship with the customer.
b) After the expiry of the relationship with the customer, such data/ information may be stored in soft copy until the expiry of the prescribed period.
c) The Company shall make available the identification records and transaction data to the competent authorities upon request;
d) The Company shall introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
e) The Company shall 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.

11 Reporting of Transactions

11.1 Internal reporting of compliance with the Policy

Report	Party to Report	Time Period
Report on Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk.	Board	Annually
Update on regulatriy changes on KYC/ AML	Board	Ad hoc
Submission of quarterly audit notes and compliance	Audit Committee/ Board	Quarterly

11.2 Reporting of specified transactions to FIU-IND

The Principal Officer of the Company has been entrusted with the responsibility of collating and reporting transactions prescribed under the PMLA and the Rules.

Principal Officer must submit Suspicious Transaction Report (STR)/ with Financial Intelligence Unit-India (FIU-IND) in the circumstances when the Company believes that it would no longer be satisfied that it knows the true identity of the customer and/ or where appropriate CDD measures not applied.

The information to Director, FIU-IND shall be reported in the prescribed formats and within the statutory time period in respect of the specified transactions in the following manner:

Report	Time Period
Cash Transaction Report (CTR) for each month	Every month by the 15th day of the succeeding month.
Suspicious Transaction Report (STR)	Immediately on arriving at a conclusion that any transaction, or a series of transactions integrally connected are of a suspicious nature but not later than seven working days on being satisfied that the transaction is suspicious.
Transction with people mentioned in Designated List issued by Ministry of Home Affairs	The Company shall not carry out any transaction with the entities/individual match with the particulars of designated list and in case of match, immediately inform the transaction details *to* the FIU-IND by email, FAX and by post, without delay

However, it should be ensured that there is no tipping off to the customer at any level in respect

of STR.

11.3 Responding to alerts shared by FIU-IND and law enforcing agencies

Certain information is sought by FIU or police authorities by way of notice or alerts. The relevant information from Company database including customer detail, customer transaction detail, etc. shall be reported to the concerned authorities within prescribed time period and format, if any.

11.4 Submission of Customer's Information to CKYCR

The Company shall apply for and obtain registration with CKYCR for sharing the requisite customer's data available with the Company with CERSAI in terms of the provisions of the Rules..

The Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer. The Company shall follow operational guidelines for uploading the KYC data as issued and amended by CERSAI time to time.

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

Whenever the Company obtains additional or updated information from any customer, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR.

CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Company.

11.5 Reporting on Non-Profit Organisations

In case, the Company has customers who are non-profit organisations, the Company shall register details of such customers on the DARPAN Portal of NITI Aayog.

11.6 Reporting on KYC Compliance Status to RBI

Company needs to ensure timely or periodic, as the case may be, submission of other ad-hoc reports, if any, to the RBI, as may be sought from time to time.

12 Training

12.1 Employee Training and Awareness on KYC Compliances

The Company should have in place an adequate screening mechanism as an integral part of their personnel recruitment/ hiring process. The Company must have an ongoing employee training programme so that the employees are adequately trained in KYC/AML.CFT policy and procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers.

Further, the employees must be trained to

a) educate/ inform the customers about the KYC/AML/CFT procedures, need for documents, information etc. and also to deal with the customer who raises issues in sharing such information. It is crucial that all those concerned fully understand the rationale behind the KYC/AML/CFT policies and implement them consistently.
b) The employees of the Company should immediately report a transaction they find suspicious, or involving money laundering activity, or in violation of KYC Norms to the designated officers of the Company.

12.2 Employee Training and Awareness on Money Laundering aspects

The Company employees including front-line staff, service provider agents and distributors, as applicable, should be trained on money laundering aspects, including without limitation:

a) money laundering tendencies noticed by them during their interaction with Customers, specifically in case of field investigation/ verification employees/ partners
b) noticeable suspicious behaviour of customers
c) cover case studies on suspected behaviours
d) for sales employees, repercussions of not disclosing suspected customer information/ behaviour, tipping off customers and assisting the Customers to circumvent thresholds for reporting.
e) Money laundering trends in the financial sector to help identify launderers in day to day transactions

The training of employees and agents, both induction as well as refresher trainings, should be conducted on an ongoing basis, and may be customised based on the roles of the employees and level of customer interaction.

Special Training, wherever required, in case of persons directly connected with the core operations such as KYC verification, credit and risk teams etc, may be imparted to make them understand the reporting processes and kind of data required reporting purposes.

13 Exit Procedures

The Company shall follow the below exit procedure as per the customer category specified below:

Sr. No.	Event type	Exit Procedure
1	Failure to furnish valid identity and address proof document as per this Policy	In case the customer fails to submit the required valid identity and address proof document despite repeated attempts by the Company, (a) The Company shall temporarily cease operations in the account and all the loans of

		such customer shall be recalled by the Company; and (b) non-compliant customers shall be barred from doing any further business with the Company until completion of KYC or periodic updation, as the case may be. Explanation: "Temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer submits the required documents. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.
2	Unacceptable High-Risk Customer – during CDD	In case the Customer has been rated as 'Unacceptable' during CDD measures applicable at the time of on boarding, then the Customer will not be on-boarded.
3	Change in Risk Categorisation of existing Customer to Unacceptable High Risk	In the event of an existing customer, or the beneficial owner of an existing customer (wherever applicable) with low/ medium risk, subsequently becomes an Unacceptable High Risk customer, the Company shall immediately cease relationship with such customers and intimate the customers as per Company policy unless prohibited under law. The Company shall also ensure requisite reporting to specified authorities.

Annexure 1

Anti – Money Laundering Risk categorisation of customers

A. Unacceptable High Risk Customers

i. Persons - Individuals involved, or suspected to be involved, in fraud against the Company and/ or its customers falling under Screening List, Individuals with dubious reputation as per public information available or commercially available watch lists; Individuals named under Screening List, High Net Worth individuals etc

ii. Occupation/ business/ professions – persons involved in the business which are considered unacceptable by the Company like, arm manufacturers/ dealers, real estate developer, gambling and gaming, money lender etc.

iii. Purposes - persons availing the loan for the purposes which are considered unacceptable by the Company like investments in shares, purchase of arms, lottery, gambling etc

iv. Non-individual customers - Firms including partnership/ proprietorship firms, Companies, body corporates, Complex business ownership structures to conceal underlying beneficiaries, Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations, or multi-level marketing companies; Client Accounts managed by professionals such as accountants or lawyers

B. Acceptable High Risk Customers

i. Non-face-to-face individuals, not being unacceptable high risk customers, acquired through Digital Lending Platforms/ Channels.

ii. Customers categorised as High-Risk basis the customer risk categorisation model implemented by the Company

C. Medium/ Low Risk Customers

i. Customers categorised as Medium or Low Risk basis the customer risk categorisation model implemented by the Company

Annexure 2

Information/ document required from individual customers

1. For undertaking CDD, the Company shall obtain the following information from an individual Customer while establishing an account-based relationship with the Company:
   a. A copy of the identity and address proof of the individual Customer. The proof shall be the document provided in the list of Officially Valid Document ("OVD") issued by RBI from time to time, or an equivalent electronic document ("e-document") of any 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.
   b. The Permanent Account Number (PAN) of the Customer shall be collected.

2. Where the customer has submitted Aadhaar as OVD,

a. the Company may carry out offline verification of Aadhaar through such modes as specified by RBI

b. the Company shall ensure that the Aadhaar number is redacted or blacked out through appropriate means.

3. List of Officially Valid Documents approved by RBI – Apart from Aadhaar, the Company may obtain any of the following documents as identity or address proof to the extent such document may be verified through the online database provided by the Government of India or its authorised entity, or the document is avaiable in an equivalent e-document form digital signed by the concerned authority as per the provisions of the Information Technology Act, 2000 and any rules issued thereunder, or the document can be downloaded from CKYCR.

- Driving license
- NREGA Job Card duly signed by an officer of State Government
- Passport,
- Voter's Identity Card issued by Election Commission of India,
- Letter issued by National Population Register containing detail of name and address