



ORANGE RETAIL FINANCE INDIA PRIVATE LIMITED

**POLICY ON KNOW YOUR CUSTOMER (KYC) / ANTI
MONEY LAUNDERING (AML) MEASURES**

APPROVAL AUTHORITY:

Document Classification	External
Created by	Compliance Department
Reviewed by	Risk Management Committee
Approved by	Board of Directors of the Company

Policy on Know Your Customer/Anti-Money Laundering Measures

Table of Contents

Sr. No	Contents
1	Introduction
2	Regulatory Requirement
3	Objectives and Scope of Policy
4	Applicability
5	Definitions
6	Compliance of KYC Policy
7	Key Elements
8	Customer Acceptance Policy (CAP)
9	Risk management
10	Customer Identification Procedure (CIP)
11	Customer Profile
12	Customer Education
13	Customer Due Diligence Procedures (CDD)
14	Risk record Management (RRM) and Monitoring of Transactions
15	Money Laundering and Terrorist Financing Risk Management
16	Identification
17	Verification
18	Maintenance of Records of Transactions & Identity
19	Preservation of Records
20	Central KYC Registry (CKYCR)
21	Accounts of Politically Exposed Persons (PEPs)
22	Appointment of Designated Director
23	Appointment of Principal Officer
24	Reporting Requirements to Financial Intelligence Unit – India (FIU-IND)
25	Confidentiality of Information
26	Hiring of Employees and Employee Training
27	Investors KYC Policy
28	Amendment
Annexure I	Indicative list for Risk Categorizations
Annexure II	Customer Identification Procedure – the documents that may be obtained from borrowers/investors

Policy On Know Your Customer (KYC) / Anti Money Laundering (AML) Measures

1. Introduction

Orange Retail Finance India Private Limited is a non-banking financial company ("NBFC") with a valid certificate of registration from the Reserve Bank of India ("RBI"). It falls under the Base Layer as per Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023.

Founded in 2014, Orange Retail Finance India Private Limited ("Company") is engaged in the business of financing two wheelers and Secured MSME Loans (LAP) in South India with a network of 50+ branches.

2. Regulatory Requirement

The "Know Your Customer" ("**KYC**") guidelines issued by the Reserve Bank Of India ("**RBI**") (RBI /DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016) as updated from time to time aims at preventing Non-Banking Finance Companies ("**NBFCs**") from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism. Accordingly, in compliance with the guidelines issued by RBI regularly, the Policy on Know Your Customer (KYC)/ Anti-Money Laundering (AML) Measures ("**Policy**") of **Company** is hereby formulated and approved by its Board of Directors ("**Board**").

3. Objectives and Scope of Policy

- To prevent criminal elements from using the Company for money laundering activities.
- To lay down explicit criteria for acceptance of customers.
- To establish procedures to verify the bona-fide identification of individuals/ non individuals before becoming an account holder/customer.
- To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To establish processes and procedures (of verification for / to monitor) of Customer Acceptance Process, Customer Identification Process, Risk Classification Process and Transaction Monitoring Process.

- To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures in respect of customers identification and reporting of such transactions.
- To develop measures for conducting due diligence.
- To comply with applicable laws and regulatory guidelines.

4. Applicability

This Policy is applicable to all products offered by the Company and all its offices and branches. This Policy is also applicable to all persons who are acting as agents of the Company.

5. Definitions

- "Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
- "Account"** includes borrowings by and from the Company.
- "Act"** and **"Rules"** means the Prevention of Money-laundering Act, 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto. Together the Act and the Rules are referred to as PMLA.
- "Beneficial Owner"** in relation to a customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the customer. A list of persons who are to be considered as such BOs in relation to a customer is given below: -

Type of Customer	Persons to be considered Beneficial Owners (BOs)
Public /Private Limited Companies	<ol style="list-style-type: none"> A natural person having, whether alone or together, or through one or more juridical person, ownership of or entitlement to more than ten percent of shares or capital or profits of the Company; or A natural person having, whether alone or together, or through one or more juridical person, right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements; or Where none of the above is been identified – a natural person who holds the position of senior managing official.

Partnership Firm	<p>a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than ten percent of capital or profits of the partnership; or</p> <p>b) Where the above is not been identified – a natural person who holds the position of senior managing official</p>
Unincorporated association of persons or body of individuals	<p>a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than fifteen percent of property or capital or profits of such association or body of individuals; or</p> <p>b) Where the above is not been identified – a natural person who holds the position of senior managing official.</p>

Trust/ Foundation	<ul style="list-style-type: none"> a) The Author of the trust; or b) The Trustees of the trust; or c) The Beneficiaries of the trust with ten percent or more interest in the trust; or d) A natural person exercising ultimate effective control over the trust through a chain of control or ownership.
<p>Exemption from identification of BO: It is not necessary to identify and verify the identity of any shareholder or beneficial owner of an entity where the customer or the owner of the controlling interest is:-</p> <ul style="list-style-type: none"> (i) an entity listed on a stock exchange in India, or (ii) 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 listed entities. 	

- e. **"Customer"** means a person who is engaged in a transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
For the purpose of this Policy, a "customer" will include the following:
 - a) A person or entity who is engaged in financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting (i.e., the beneficial owner);
 - b) Beneficiaries of transactions conducted by professional intermediaries such as Stock- brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law; or
 - c) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company. e.g., a wire transfer or issue of a high value demand draft as a single transaction.
 - d) A past as well as prospective customer having attempted or executed transactions.
- f. **"Customer Acceptance Policy"** shall have the same meaning as specified in clause 8 of this Policy.
- g. **"Customer Due Diligence" or "CDD"** means identifying and verifying the customer as defined in clause (e) of this Policy using reliable and independent sources of identification.
- h. **"Customer Identification"** means undertaking the process of CDD.
- i. **"Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

- j. **"Designated Director"** means the Managing Director or whole time Director duly authorized by Board of Directors to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules.
- k. **"Digital KYC"** means the capturing live photo of the client 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 reporting entity as per the provisions contained in the Act.
- l. **"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.
- m. **"Know Your Customer Identifier"** means the unique number or code assigned to a client by the Central KYC Records Registry.
- n. **"Know Your Customer Records"** means all records, documents and information constituting the basis for carrying out the Customer Due Diligence procedures in accordance with Rule 9 of the Rules.
- o. **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- p. **"Last KYC verification or updation"** means last transaction made in the CKYC records registry by which the KYC records of a customer were recorded, changed or updated.
- q. **"Money Laundering"** shall have the same meaning as defined under section 3 of the Prevention of Money - laundering Act, 2002 for the time being in force.
- r. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.
- s. **"Non-Profit Organization"** means any entity, organization, society, trust, company or any other institution incorporated or constituted for religious or charitable purposes as referred to in section 2 (15) of the Income Tax Act, 1961 and includes all entities and institutions registered U/s 8 of the Company Act, 2013, Society Registration Act, 1860, Maharashtra Public Trusts Act, 1950 or any other legislation governing and regulating the affairs of such institutions for the time being in force in any part of the Territory of India.

- t. **"Officially Valid Document" ("OVD")** means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that
- a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
 - b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
 - utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - Property or municipal tax receipt;
 - Pension or family payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;
 - c) The customer shall submit OVD with current address with a period of three months of submitting the documents specified as above.
 - d) (as and when applicable) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
- u. **"On-going Due Diligence"** means Due Diligence of the customers undertaken to ensure the transactions with the customers are consistent with the knowledge about the customers, customer business, risk profile and the source of funds.
- v. **"Principal Officer"** means an officer at the management level nominated by the Company responsible for furnishing information as per rule 8 of the Rules
- w. **"Senior Management"** as defined in Nomination and Remuneration Policy of the Company.
- x. **"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 Terrorist Financing.
- y. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes -
- opening of an account;
 - deposits or transfer of funds, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means;
 - the use of a safety deposit box or any other form of safe deposit;
 - entering into any fiduciary relationship;
 - any payment made or received in whole or in part of any contractual or other legal obligation;
 - establishing or creating a legal person or legal arrangement.
- z. **"Terrorist financing"** is the financing of terrorist acts, terrorists and terrorist organizations.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the RBI Guidelines and other regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6. Compliance of KYC Policy

The Company's senior management team comprising of respective vertical heads oversee KYC compliance in line with the Policy. The Internal Audit team shall on a continuous basis conduct an independent evaluation of adherence to KYC compliance requirements and submit audit notes and report on compliance to Audit Committee on quarterly basis. The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

7. Key Elements

KYC procedures also enable the Company to know/understand its Customers and their financial dealings better which in turn help to manage its risks prudently. We have framed the Policy incorporating the following five key elements:

- Customer Acceptance Policy ("**CAP**");
- Risk management.
- Customer Identification Procedures ("**CIP**");
- Customer Due Diligence Procedures ("**CDD**"); and
- Risk Record Management ("**RRM**")& Monitoring of transactions.

8. Customer Acceptance Policy ("**CAP**")

The Company's CAP lays down criteria for acceptance of customers. The Company shall ensure that:

- a. No account is opened in anonymous or fictitious *benami* name(s);
- b. No account shall be opened where there is an inability to apply procedures for Customer Due Diligence either due to non-co-operation of the customer or non- reliability of the documents, records, information and explanation furnished by the customer.
- c. No account based relationship shall be accepted without following the procedures as mandated in Rule 9 of the Rules.
- d. Sufficient compliance with Rule 9 and appropriate KYC records shall be sort while accepting customer account based relationship.
- e. Application of customer Due Diligence norms as per Rule 9 of the Rules at Global Customer ID level shall be undertaken while accepting customer account based relationship. However, no customer due diligence procedure shall be applied in case the existing KYC compliant customer desires to avail other services in addition to the first KYC compliant service.
- f. In the case of joint accounts, separate customer due diligence procedures shall be undertaken for all the joint account holder in accordance with the Rule 9 of the Rules.
- g. No service shall be denied to any customer on the ground that the customer does not have Aadhaar number in accordance with section 11 A(3) of the Act. In such a case, other KYC compliance procedure shall be observed.
- h. Evaluate the circumstances in which the customer is permitted to act behalf of another person or entity.

- i. Suitable measures shall be stipulated for identification of customers whose name matches with the name of any person or entity notified under Chapter IX Master Direction – Know Your Customer (KYC) Direction, 2016.
- j. Adequate steps shall be taken to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, sanctioned persons;
- k. No account will be open as non- face to face customer.
- l. Verification of customer records such as PAN, GST registration certificates or any other equivalent e-documents shall be undertaken in accordance with the verification facilities provided by the issuing authorities as well as digital signatures as per the Information Technology Act, 2000.
- m. Customer Acceptance Policy shall not result in denial of services to the general public especially those belonging to financially and socially disadvantaged individuals.
- n. If the Company is suspicious of money laundering or terrorist financing, and reasonably believes that performing the Customer Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report (STR) to FIU-IND.

In case of Inactive Prospective Customers (who do not approaches to the Company) the Company will auto-cancelled the case after 30 days of application creation date and data will store in the system. Application status will be mark as auto-cancelled.

9. Risk Management

The Company shall have risk based approach for management and mitigation of risk comprising the following:

- 1. The risk categorization of the customers shall be undertaken on the parameters such as customer's identity, occupation, social and financial status, location, nature of business activity, geographical risk covering customers as well as transaction, types of products and services offered and mode of payment as well as receipts.
- 2. While considering customer's identity, the ability to verify and confirm officially valid documents to the facilities providing by the issuing authorities shall also be taken into account.
- 3. Customers shall be categorized by low, medium and high risk based on the assessment and risk perception norms stipulated by the Company.
- 4. Broad principles shall be identified and stipulated for appropriate risk categorization of the customers. An indicative risk categorization for general guidance is provided in Annexure I.
- 5. The risk categorization of the customer and the specific reasons for such categorization shall be kept confidential, and shall never be revealed to any customer to avoid tipping off to any customer.

10. Customer Identification Procedure ("CIP")

Customer identification means identifying the Customer and verifying his/her/its identity by using reliable, independent source documents, data or information. The customer Identification procedures shall be undertaken in the following circumstances:

1. At the time of commencement of account based relationship with the customers.
2. When there is doubt about the authenticity and adequacy of the customer identification data available with the Company.
3. Selling products through third parties such as agents and brokers involving value exceeding rupees 50,000.
4. When there is a reason to believe that a customer is intentionally structuring a transaction into a series of multiple transaction below the threshold limit of rupees 50,000.00.
5. Where the introduction shall not be insisted upon while accepting customer account based relationship.
6. Maintain records of the information used to verify a Customer's identity, including name, address and other identifying information
7. Consult Sanctions Lists/ Financial Actions Task Force ("**FATF**") /Office of Foreign Control Assets ("**OFAC** ") databases for known or suspected terrorists or terrorist organizations
/jurisdictions and countries that do not or insufficiently apply the FATF recommendations as provided to the Company by RBI or any other applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.

11. Customer Profile

For the purpose of exercising due diligence on individual transactions in accounts, a 'Customer Profile' of individual Customers is included in the loan application. The customer profile will contain information relating to the Customer's identity, social/ financial status, information about the Customer's clients' business and their location etc. The information will be of two types namely mandatory and optional as stated below:

(a) Mandatory Information:

(i) Identity (ii) Address (iii) Occupation (iv) Source of funds (v) Monthly Income (vi) Annual turnover (vii) Date of Birth (viii) Assets (approximate value).

(b) Optional Information:

(i) Marital Status; (ii) Educational Qualification; (iii) Details of spouse; (iv) Details regarding children; (v) Other Information which can include queries on a) Car/two-wheeler ownership,
b) has a credit card c) has an insurance Policy.

The Company shall, where its Customer submits a proof of possession of Aadhaar Card containing Aadhaar Number, ensure redacts or blacks out of his Aadhaar number is done through appropriate means.

12. Customer Education

The Company will take adequate measures to educate the Customers on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the Customers. When required to collect any information about the Customer for the purpose other than KYC requirement, it will not form part of the loan application. Such information will be collected separately, purely on a voluntary basis in a form prescribed by the Company after explaining the objective to the Customer and taking the Customer's express approval for the specific uses to which such information could be used. The customer servicing staff is specially trained to handle such situations while dealing with Customers. The Company takes care to see that implementation of the KYC guidelines in respect of customer acceptance, identification etc. do not result in denial of opening of new loan accounts to public.

13. Customer Due Diligence Procedures ("CDD")

1. The Company shall perform CDD procedures for accepting account based relationship with customers, identification of beneficial owners, ongoing due diligence and periodic updation of KYC records.
2. In addition to above, the Company shall not onboard non-face to face customers and politically exposed person.
3. Adequate CDD procedures would be deployed by the Company in respect of accounts opened by professional intermediaries on behalf of clients.

Ongoing Due Diligence

Ongoing monitoring is an essential element of effective KYC procedures. The Company effectively controls and reduces the risk through understanding of the normal and reasonable activity of the Customer and by it having the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The Company should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts will be subjected to intensify monitoring.

Illustrative list of activities which is construed as suspicious transactions

- Activities not consistent with the Customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid reporting/record-keeping requirements/provide insufficient/ suspicious information:
- A Customer who is reluctant to provide information needed for a

mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

- Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
- Certain employees of the Company arousing suspicion:
 - An employee whose lifestyle is beyond his/her economic means
 - Negligence of employees/willful blindness is reported repeatedly.
- Multiple accounts under the same name.
- Refusal to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.
- There are reasonable doubts over the real beneficiary of the loan.
- Frequent requests for change of address.

The company may adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

Review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation shall not be less than once in ten years in case of low risk category customers, not be less than once in five years in case of medium risk category customers and not less than once in two years in case of high risk categories in the following manner. The Company shall ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk.

1. Individual customers	
a) No change in KYC information	A self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.
b) Change in address	A self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of Company),

	letter etc. the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.
--	--

<p>2. CUSTOMERS OTHER THAN INDIVIDUALS (LEGAL ENTITY)</p> <p>a) No change in KYC information</p> <p>b) Change in KYC information</p>	<p>A self-declaration shall be obtained from the Legal Entity (LE) customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. The Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.</p> <p>The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.</p>
--	---

<p>3. ADDITIONAL MEASURES</p>	<ul style="list-style-type: none"> a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer. b) Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC. c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self- declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer. d) In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC through online portal as well as at branch level. e) The Company shall adopt a risk based approach with respect to periodic updation of KYC.
<p>4. OBLIGATIONS OF CUSTOMERS:</p>	<p>The Customers are required to submit the updated KYC documents to the Company, in case of any updation in the KYC already submitted by the customer at the time of establishment of business relationship / account- based relationship and thereafter, as necessary, within a period of 30 days from such update in order to comply with the PML Rules.</p>

Enhanced Due Diligence

Enhanced Due Diligence will involve closely monitoring the account, frequently updating KYC documents, field investigation or visiting the customer, etc., which forms part of the credit policies of the businesses.

if the Company has Customers or accounts that are determined to pose a potential high risk and thereby warrant enhanced scrutiny then it shall conduct Enhanced Due Diligence in connection with such Customers. The Company has established appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the Company as per the procedures stipulated by Reserve Bank of India in Master Direction (KYC), 2016 (DBR.AM.BC.81/14.01.001/2015-16 dated 25.02.2016) as amended from time to time.

The following are the indicative list where the risk perception of a Customer which is considered higher:

- Customers requesting for frequent change of address/contact details;
- Sudden change in the loan account activity of the customers; or
- Frequent closure and opening of loan accounts by the customers.

In case of sale of repossessed vehicles by company to purchasers/brokers, company shall ensure to collect the KYC (Identity & address proof) so as to ensure the real identity of the buyer of such repossessed vehicles. Company shall obtain a declaration from the buyer that vehicles are being sold by the Company on 'As is Where Is' basis and the buyer is responsible to ensure the name transfer in RTO Records and deletion of the Company's hypothecation thereon. This ensures Company / its original customers is not accountable for repossessed vehicles being used for terrorist or any other unlawful activities.

The Company obtains End Use Declaration letter from customers confirming the purpose of finance taken and a declaration that the Facility shall not be used for any illegal and /or anti- social and / or speculative purposes including but not limited to participation in stock markets / IPOs.

14. Risk Record Management ("RRM") and Monitoring of Transactions:

- 1) The Board of Directors ("Board") of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles and principles for risk categorization of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

- 2) The Company shall abide by the provisions of Rules made in this behalf by the competent authorities.
- 3) In accordance with section 12 of the Act, the Company shall maintain and preserve the records pertaining to the customer due diligence and transaction monitoring upto the time limit of five (5) years as prescribed in that section.
- 4) The Company shall deploy physical as well as electronic systems for maintenance of proper records in relation to transactions reportable in Rule 3 of the Rules. The information contain in the records shall be sufficient to permit reconstruction of individual transactions comprising:
 - a. Nature of the transactions;
 - b. The amount of transaction and currency in which it was denominated;
 - c. Date on which the transaction was conducted;
 - d. Parties to the transactions.
- 5) The Company shall evolve a system for proper maintenance and preservation of customer and account related information in a manner that allows easy retrieval as and when requested by the competent authorities.
- 6) While obtaining and preserving the customer records, the Company shall abide by the provisions of Digital Personal Data Protection Act, 2023 and the Rules made there under.
- 7) The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers.

15. Money Laundering and Terrorist Financing Risk Assessment

- a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise regularly to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk.
- b. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.
- c. The risk assessment by the Company shall be properly documented and be commensurate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.
- d. The outcome of the exercise shall be put up to the Risk Management Committee on a quarterly basis and will be available to competent authorities and self-regulating bodies. The Company shall apply a Risk Based Approach ("**RBA**") for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

16. Identification

All customers shall be identified by a unique identification code. This unique code will be employed to track the facilities availed, monitor financial transactions which assists in risk profiling of customers. The customer identification requirement applicable to borrowers / investors are detailed in Annexure II to this Policy

17. Verification

As a part of the Lending Policy, the Company documents and implemented appropriate risk- based procedures designed to verify that it can form a reasonable belief that it knows the identity of its Customers (Borrower's). Verification of customer identity should occur before transacting with the Customer. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents, non- documentary verification methods or *additional verification procedures* that are appropriate with the associated risks, which are explained below;

I. Verification through documents:

These documents may include but are not limited to the list of documents that can be accepted as proof of identity and address from customers by the Company as provided in the Lending Policy. The customer identification requirement applicable to borrowers / investors are detailed in Annexure II to this Policy

II. Verification through non-documentary methods:

The Company depends on other methods of verification as listed below:

1. Contacting or visiting a Customer;
2. Independently verifying the Customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; or
3. Checking references with other financial institutions.

III. Additional verification procedures.

The Business Head advises the credit team to make a personal visit to address under the following situations.

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The sales executive is not familiar with the documents presented;
3. Where the sales executive is otherwise presented with circumstances that increase the risk that it will be unable to verify the identity of a Customer through documents; and
4. If the sales executive cannot verify the identity of a Customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, to verify the customer's identity.

18. Maintenance of Records of Transactions & Identity

The Company has a system of maintaining proper record of transactions prescribed under Rule 3, of the PML Rules 2005 and value of transactions, the procedure and manner of maintaining and verification and maintenance of records of the identity of the clients as mentioned below:

- All cash transactions of the value of more than Rupees Ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below Rupees Ten lakhs 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 Rupees Ten lakhs;
- All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- As per the RBI guidelines, the Company maintains the following information in respect of transactions referred to in Rule 3 of the Rules:
 - Nature of the transactions;
 - Amount of the transaction and the mode adopted for undertaking the transaction;
 - Date on which the transaction was conducted; and
 - Parties to the transaction.

19. Preservation of Records

The Company will maintain the records containing information of all transactions including the records of transactions detailed in PML Rule 3. The Company should also take appropriate steps to evolve a system including establishment of appropriate AML / CFT Cell at HO Level for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

The Company should maintain records relating to the transactions, whether attempted or executed, in such manner & for such period as specified under section 12 of the Act.

The Company should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules. The identification records and transaction data **including attempted & executed** should be made available to the competent authorities upon request.

The Company should ensure that if its customer is a non-profit organization, it shall be registered on the DARPAN Portal of NITI Aayog. If it's not registered, then Company shall take appropriate steps to register the same and maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is late.

20. Central KYC Registry ("CKYCR")

The Company will ensure that the Customer KYC information is shared with the CKYCR in the manner mentioned in the RBI Directions in RBI's KYC templates prepared for 'Individuals' and 'Legal Entities' with Central Registry of Securitization Asset Reconstruction and Security Interest of India ("**CERSAI**") in accordance with the provisions of law and regulations for the time being in force.

21. Accounts of Politically Exposed Persons (PEPs)

- A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:
 - 1. The Company have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
 - 2. Reasonable measures are taken by the Company for establishing the source of funds / wealth;
 - 3. The approval to open an account for a PEP shall be obtained from the Senior Management;
 - 4. All such accounts are subjected to enhanced monitoring on an on-going basis;
 - 5. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Senior Management's approval is obtained to continue the business relationship;
- B. These instructions shall also be applicable to family members or close associates of PEPs.

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

22. Appointment of Designated Director

The Managing Director of the Company shall be appointed as Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and Rules.

The Company shall submit the name, designation, address and contact details of the Designated Director to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

23. Appointment of Principal Officer

The Chief Financial Officer or the Company Secretary or any other person authorized by the Board shall be appointed as Principal Officer of the Company, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under PML Act/ KYC Policy.

The Company shall submit the name, designation, address and contact details of the Principal Officer to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

24. Reporting Requirements to Financial Intelligence Unit - India (FIU-IND)

The Company is registered with FIU-IND.

The Company shall furnish the following reports to the Financial Intelligence Unit-India (FIU- IND), with regard to information referred to in Rule 3 of the Rules and in terms of Rule 7 thereof in the manner so specified and within the timelines prescribed therein;

- a. Cash Transactions Report ("**CTR**")
- b. Suspicious Transactions Report ("**STR**")
- c. Counterfeit Currency Reports ("**CCR**")
- d. Non-Profit Organization Reports ("**NPR**")

The Company has implemented a system not to accept cash of more than Rs. 2 lakhs at a time from its borrowers. Hence, it normally does not and would not have large cash transactions. However, when cash transactions monthly aggregating of more than Rs. 10 lakhs are undertaken, the Company will maintain record of all such cash transactions.

The Company monitors 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

Company depends on the risk sensitivity of the account and special attention is given to all complex unusually large transactions, which have no apparent economic or lawful purpose. The Company shall promptly report such high value cash transactions or transactions of a suspicious nature to the appropriate regulatory and investigating authorities. The Company has a system which alerts inconsistent transactions and profile of the customers is updated for effective identification and reports of suspicious transactions.

25. Confidentiality of Information

Information collected from Customers for the purpose of opening of account shall be treated as confidential and in accordance with the agreement/terms and conditions signed by the Customers. The 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. While considering the requests for data/information from Government and other agencies, the Company shall satisfy that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in their transactions.

The exceptions to the said rule shall be as under:

- a) Where disclosure is required under law;
- b) Where there is a duty under the law to disclose such information ;
- c) Where the disclosure is made with the express or implied consent of the Customer subject to the provision of Digital Personal Data Protection Act, 2023.

26. Hiring of Employees and Employee Training

The Company must have an ongoing employee training program on at least half yearly basis so that the members of the staff are adequately trained in KYC procedures. Training requirements have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

There should be open communication, high-integrity, proper understanding of subject matter amongst the Company's staff dealing with KYC/AML matters.

27. Investor KYC Policy

The Company's guidelines pertaining to four Key elements viz. Customer Acceptance Policy, Risk Management, Customer Identification Procedures, Customer Due Diligence and Risk Record Management & Monitoring of Transactions of this KYC framework, mentioned in this Policy will be equally applicable for its investors with suitable modifications depending upon the activity undertaken. The Company shall ensure that a proper framework

on KYC and anti-money laundering standards are put in place in this regard. Basic KYC shall be completed through details like Certificate of Incorporation, PAN, TIN, GST etc. All funding proposals will be subject to proper checks on OFAC/ FATF / UN Sanctions List circulated by RBI / List of Willful defaulters / Other List of Terrorist Organizations.

The FATF periodically identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in its following publications:

- a) High-Risk Jurisdictions subject to a Call for Action, and
- b) Jurisdictions under Increased Monitoring.

In compliance of RBI's Circular regarding Investment in NBFCs from FATF non-compliant jurisdictions dated February 12, 2021, the Company promotes investments from FATF compliant jurisdiction, i.e. from entities whose name does not appear in the aforementioned lists. Records of such checks shall be maintained.

28. Amendment

The Board reserves the right to amend (either in whole or in part), suspend or rescind this Policy at any time. However, no such amendment or modification will be binding on the Employees and Directors unless the same is notified to all in writing. Whilst, the Company has made best efforts to define detailed procedures for implementation of this Policy, there may be occasions when certain matters are not addressed or there may be ambiguity in the procedures. Such instances or ambiguities will be resolved in line with the broad intent of the Policy. The Company may also establish further rules and procedures, from time to time, to give effect to the intent of this Policy and further the objective of good corporate governance. The Board shall also review this Policy on a periodic basis and at least once every year.

Annexure I

Indicative list for Risk
Categorization:

Sr. No.	Low Risk (Level 1)	Medium Risk (Level 2)	High Risk (Level 3)
1.	Students, Housewives, Pensioners.	Non-Banking Financial Institutions.	Politically Exposed Persons & their relatives.
2.	Salaried Persons	Credit Co-Operative Societies	Jewelers & Bullion Dealers
3.	Shareholders of the company	Non-Scheduled UCBs	Accounts of construction & real estate dealers & brokers
4.	Small Traders	Travel Agents	Trusts / NGOs / Organizations receiving donations
5.	Self-Employed	Dealers in Pharmaceuticals	Persons with dubious reputation, knowledge of which is available in public domain
6.	Self Help Groups	Dealers of Wholesale electronic materials	Accounts, being subject to investigation by law enforcement agencies.
7.	Staff & their relative accounts	Advocates, Solicitors & Notaries	Names 100% matching with the Persons notified by UNSC.
8.	Co-Operative Housing Societies	Dealers in new as well as used two wheelers	Persons with criminal background, knowledge of which is available in public domain.
9.	Professionals such as CA, CS,CMA, Doctors, Engineers, Consultants	Used car sellers	Dealers in antiques
10.	Agricultural & allied activities	Dot Com Companies or internet service providers	Dealers in arms
11.		Auctioneers	Share brokers
12.		Restaurants & Bar	Unclaimed deposit accounts
13.		Telemarketers & Telecommunication service providers	Money Changes / Remitters
14.		Internet Café	New opened accounts for first 6 months

15.		IDD Call Service Providers	KYC Non-Compliant Accounts
16.			Firms with sleeping partners
17.			HNI Customers
18.			Customers appearing to be Multi-Level Marketing Companies
19.			Clients managed by professional service providers such as law firms, accountants, brokers, etc.
20.			Customers with High Net Worth (above Rs.1 Crore)

Annexure II

Customer Identification Procedure –
The documents that may be obtained from
borrowers/investors:

Nature of customer	List of applicable documents
Individual	<p>The Company shall obtain the following from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:</p> <ul style="list-style-type: none">a) a certified copy of any OVD containing details of his identity and address; andb) the Permanent Account Number (PAN) or Form no.60; andc) One recent photographd) Such other documents as specified by the Company from time to time.e) the KYC Identifier with an explicit consent to download records from CKYCR. <p>List of OVDs:</p> <ul style="list-style-type: none">i) Passport,ii) Driving licenseiii) Proof of possession of Aadhaar numberiv) Voter's identity card issued by the Election Commission of Indiav) Job card issued by NREGA duly signed by an officer of the State Govt.vi) Letter issued by the National Population Register containing details of name and address. <p>Provided that:</p> <ul style="list-style-type: none">1) 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 UIDAI.2) 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:-<ul style="list-style-type: none">i) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);ii) Property or Municipal tax receipt;iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;iv) Letter of allotment of accommodation from employer issued by State Govt. or Central Govt. Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies

and leave and licence agreements with such employers allotting official accommodation.

The Credit Head of The Company has the power to approve the following documents in lieu of ID and address proof.

In lieu of Identity proof

Notarized copy of Marriage certificate with the applicant photograph. Explanation: A document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name

In lieu of address proof

- ✓ Rental agreement along with rent receipt and utility bill of the Landlord.
- ✓ In case the customer has a temporary address being a transit arrangement provided by real estate builder – Allotment letter issued by the builder + permanent address proof
- ✓ In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by a close relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address.

3. The Credit Head of The Company jointly with the concerned Sales Head has further delegated the approval powers to accept the above documents to credit managers, as they may deem fit and necessary, in this regard.

4. In the event of any genuine reason for non-availability of any of the prescribed documents or to approve any deviations for change in the documents prescribed under this Policy, the Credit Head jointly with the Sales Head considers approving any other document not stated above based on the product, market requirements and also on the merits of the case.

Identification number:

1. A taxpayer identification number; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAAR number; or number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise;

2. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but business

	<p>process has implemented procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period before disbursal of loan.</p> <p><i>The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above</i></p> <p>The Credit Head of The Company has the power to approve the following document in lieu of ID and address proof</p> <p><i>A Certificate from the public authority (i.e) Gazette Officer of State or Central Govt./Magistrate/MRO/VRO/Gram Panchayat Sarpanch/notary public.</i></p>
--	---

Companies	<ol style="list-style-type: none"> 1. Certificate of Incorporation, Memorandum of Association and Articles of Association 2. Resolution of the Board of Directors to open an account and identification of those who have the authority to operate the account.
-----------	---

	<ol style="list-style-type: none"> 3. Power of Attorney granted to its managers, officers or employees to transact business on its behalf 4. PAN Allotment Letter 5. Telephone Bill 6. GST number 7. Names of the relevant persons holding senior management position 8. The registered office and principal place of its business, if it is different
Partnership Firms/ LLPs	<ol style="list-style-type: none"> 1. Registration Certificate if the partnership deed is registered 2. Address of the registered office and principal place of its business, if it is different 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4. Any official valid documents identifying the partners and the persons holding the power of attorney and their addresses 5. Telephone bill in the name of firm/partners Accounts 6. PAN 7. GST number(if any)

Proprietary Concerns	<ol style="list-style-type: none"> 1. Proof of the name, address and activity of the concern like registration certificate (in case of a registered concern) including Udyam Registration Certificate (URC) issued by Government. 2. Certificate issued by the Municipal authorities under the Shops and Establishment Act, GST returns, Income Tax returns, GST Certificate, Registration documents issued by GST, Professional Tax Authorities, Certificate of Practice issued by Food and Drug Control Authorities etc. 3. Any registration documents issued in the name of the proprietary concern by the central government, state government. We also accept IEC (import-export code issued to the proprietary concern by the office of DGFT as an identity document for opening of account. 4. Income Tax return copy in the name of the sole proprietor where the firm's income is reflected duly authenticated by the Income Tax Authorities 5. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern <p>Any two of the above documents would suffice. These documents should be in the name of the proprietary concern</p>
Trusts, foundations and society	<ol style="list-style-type: none"> 1. Names of trustees, settlers, beneficiaries and signatories. 2. Names and addresses of the founder, the managers/directors and the beneficiaries. Telephone/fax numbers 3. Names of beneficial owners 4. Certificate of registration, if registered, Trust Deed, PAN or Form 60 of the Trust, Power of Attorney granted to transact business on its behalf. 5. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses

	<ol style="list-style-type: none"> 6. Resolution of the managing body of the foundation/association. 7. Telephone bill 8. the names of the beneficiaries, trustees, settlor and authors of the trust 9. the address of the registered office of the trust; and 10. list of trustees and documents, for those discharging role as trustee and authorized to transact on behalf of the trust 11. 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.
--	---

=====END OF DOCUMENT=====