KNOW YOUR CUSTOMER
& ANTI MONEY LAUNDERING POLICY

Summary of Policy:

Policy Name	Know Your Customer and Anti Money Laundering Policy
Version	8
Issue and Effective date	24.03.2026
Periodicity of Review	Annual
Owner / Contact	Credit Department
Approver	Board of Directors

Version	Date
1	24.09.2015
2	13.03.2018
3	02.09.2020
4	17.08.2021
5	06.12.2023
6	26.03.2025
7	13.08.2025
8	30.03.2026

Contents

1. PREAMBLE

Sitaara Housing Finance Limited (Formerly known as SEWA Grih Rin Limited), (hereinafter referred to as "**SITAARA**" or "**Company**") has adopted this Know Your Customer and Anti Money Laundering Policy ("**Policy**") in accordance with Reserve Bank of India (Know Your Customer) Directions, 2025 as amended from time to time ("**Master Directions on KYC**") and various circulars/ directions/ notifications as issued by Reserve Bank of India ("**RBI**") or National Housing Bank ("**NHB**") or any other appropriate authority. This is a Board approved policy.

2. PREFACE

This document details the Know Your Customer ("**KYC**") guidelines and Anti-Money Laundering ("**AML**") guidelines to be followed by the Company upon due approval by the Board of Directors or any Committee of the Board to which such power has been delegated. This Policy will be reviewed annually or based on any material change in the regulatory requirements or business operations of the Company.

The Policy & measures will enable the Company to establish a regulatory mechanism to know and understand its customers and their financial dealings, which in turn, will help the Company to manage risks prudently and ensure compliance. The Policy will also help in protecting company's reputation and preventing the company from being used, intentionally or unintentionally by unscrupulous and criminal elements for money laundering activities.

Following are the four key elements of the policy:

A. Customer Acceptance Policy;
B. Risk Management
C. Customer Identification Procedures (CIP); and
D. Monitoring of Transactions;

This KYC Policy framed hereunder is to be read and followed in conjunction with Know Your Customer (KYC) Direction, 2025, as amended and updated by RBI from time to time and any other applicable law in force. The Policy also seeks to implement mutatis mutandis, the provisions of the Prevention of Money-Laundering Act, 2002, and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

3. APPLICABILITY

The Policy is applicable to all employees, vendors, agents, applicants, borrowers, customers and persons associated with SITAARA.

Failure to adhere to this Policy may subject employees to disciplinary action, including termination of employment. The employees who suspect unethical behavior should refer the matter to appropriate personnel as directed by their business policies and procedures.

4. DEFINITIONS

i. **Aadhar number**: As defined under The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and means an identification number issued to an individual on receipt of the demographic information and biometric information, the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual.

ii. "**Customer**" means:
A person who is engaged in a financial transaction or activity with SITAARA and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting (i.e. the beneficial owner); beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law, and any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company.

iii. **Certified Copy**: Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Company as per the provisions contained in the Prevention of Money-Laundering Act, 2002.

Provided that in case of Non-Resident Indians ("**NRIs**") and Persons of Indian Origin ("**PIOs**"), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- Authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- Branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

iv. **Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) (aa) of the Prevention of Money Laundering Rules, 2005 (as amended from time to time) to receive, store, safeguard and retrieve the KYC records in digital form of a customer;

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

vi. "**Customer Identification"** means undertaking the process of CDD.

vii. "**Designated Director**" means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors of SITAARA.

viii. "**Digital KYC**" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of Sitaara as per the provisions contained in the Prevention of Money-Laundering Act, 2002.

ix. "**Know Your Client (KYC) Identifier**" means the unique number or code assigned to a customer by the Central KYC Records Registry.

x. "**KYC Templates**" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

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

xii. "**Officially Valid Document**" or OVD refers to passport, 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 her proof of possession of Aadhaar number as an OVD, she 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: -

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; and

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector

undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.
c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.
Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiii. "**Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xiv. "**On-going Due Diligence**" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers risk profile and source of funds.

xv. "**Periodic Updation**" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank of India.

xvi. "**Politically Exposed Persons**" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country e.g., Heads of States/ Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

xvii. "**Principal Officer**" means an officer nominated by company, responsible for furnishing information as per rule 8 of the Rules.

xviii. "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to not have economic rationale or bona-fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

xix. "**Transaction**" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
a. opening of an account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means;

c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

xx. **"Video based Customer Identification Process (V-CIP**)": A method of customer identification by an official of company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

For the purpose of this policy, any reference to any legislation or law or to any provision thereof shall include references to any such law as it may, after the date hereof, from time to time, be amended, supplemented or re-enacted, and any reference to a statutory provision shall include any subordinate legislation made from time to time under that provision.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, 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.

5. COMPLIANCE BY COMPANY:

In order to comply with the directions issued by Department of Revenue, Ministry of Finance, as also Reserve Bank of India issued from time to time pertaining to Know your customer and Anti-money laundering, the Company shall do the following:

a) Following officials who would form part of the Senior Management will be responsible for ensuring KYC compliance in the organization:

   i. Designated Director
   ii. National Sales Manager
   iii. National Credit Manager
   iv. Head of Operations

b) The Company shall allocate responsibility for effective implementation of policies and procedures.

c) The company shall undertake independent evaluation of the compliance functions of policies and procedures, including legal and regulatory requirements.
d) The company shall develop an internal audit system to verify the compliance with KYC/AML policies and procedures.
e) Submission of quarterly audit notes and compliance to the Audit Committee. Quarterly Audit Reports will be submitted to the Audit Committee of the Board on KYC / AML compliances in the Company.
f) The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

6. DESIGNATED DIRECTOR

The board of the company shall nominate one of the directors of the company as 'Designated director' to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The company shall communicate the name, designation and address of the Designated director to FIU-IND (Financial Intelligence Unit, Department of Revenue, Ministry of Finance, GoI). Designated Director should be different from the principal officer as designated by the company.

The Company has appointed the following person as the "Designated Director":	
Name:	Mr. Ajesh Appukuttan
Designation	Managing Director and CEO
Mail id:	ajesh.a@sgrlimited.in
Mobile No.	+91 9841040729

Key Responsibilities of the Designated Director are:

- Review the reports to be submitted to FIU.
- Ensure compliance to guidelines issued.
- Attend meetings/conferences organized by FIU or other regulatory bodies.

7. PRINCIPAL OFFICER

The Company shall designate a 'Principal Officer' in the Company. Principal Officer shall be located at the Company's Registered/ Head Office and will be responsible for furnishing the following information envisaged under the PML (Maintenance of Records) Rules 2005:

- all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

- all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
- all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;
- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
- all suspicious transactions whether or not made in cash and by way of deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:
    - cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
    - travellers cheques, or
    - transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
    - any other mode in whatsoever name it is referred to.

The Company has appointed the following Principal Officer:

Name: Ms. Suvrata Mishra
Designation: Head of Centralized Operations
Contact details: +91 9717703154

8. CUSTOMER ACCEPTANCE POLICY

The Customer Acceptance Policy (CAP) of the Company lays down the criteria for the acceptance of Customers in line with the RBI's Master Direction - Know Your Customer (KYC) Direction, 2025 as amended from time to time. The Company shall ensure that the Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged. The Company will follow the below mentioned measures in respect of its customers:

- Any person willing to either apply for a loan from the Company or has any kind of financial transaction, his/her relatives, people who are part of loan structure as per the credit policy of the Company and the co-applicant are considered as Customers and therefore may be subjected to KYC verification;
- No account shall be opened or no loans shall be disbursed to any anonymous/fictitious/benami customer or any other person whose identity has not been disclosed or cannot be verified;

- No account shall be opened and no transaction or account-based relationship shall be undertaken where the Company is unable to apply appropriate customer due diligence measures (CDD measures) i.e., the Company is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the applicant / customer or non-reliability of the information/ information furnished by such applicant/customer. Further, the Company may file STR, if necessary, when the Company is unable to comply with the relevant CDD measure.
- The above mentioned CDD measures shall be applicable for all the joint account holders, while opening a joint account;
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out;
- The mandatory information shall be sought from the Customer(s) along with optional/additional information for KYC purpose prior to opening an account and during periodic updation;
- Any additional information may be obtained with explicit consent of the customer after the account is opened;
- The Permanent Account Number (PAN) of the Customer, if obtained, shall be verified from the verification facility of the issuing authority.
    - In case an e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
    - If an existing KYC compliant customer of the company desires to open another account with the company, there shall be no need for a fresh CDD exercise;
- Documentation requirements and other information will be collected in respect of different categories of customers depending on perceived risk and requirements of Prevention of Money Laundering Act, 2002 & RBI rules framed there under and guidelines issued from time to time. Further the documents or e-documents collected shall be verified from sighting of the original documents or else by verification from facility of the issuing authority or any other reliable data source as mandated by the competent authority;
- Necessary checks will be applied before opening an account to ensure that the identity of the customer does not match with any person with a known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. or whose name appears in the “Sanctions Lists” circulated by Reserve Bank of India. Full details of accounts/ customers bearing resemblance with any of the individuals/entities in the list shall be treated as suspicious and reported.
- The customer profile prepared by company will contain information relating to the customer's identity, social / financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile only such information will be taken from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other similar purposes. However, the customer profile may be shared with a Credit Bureau, empanelled vendors subject to the confidentiality clause and / or other agencies as required by law;
- In case the Customer is unable to be present at the branch location physically, necessary checks will be done prior to disbursement of the loan through the company's designated officers or an agency appointed by the Company to ensure the identity and contact details of the customer;

- At the time of any part or full prepayment of the loan by customers a declaration will be obtained from such customers to ascertain the source of the funds which are being paid to the Company.
- 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 may consider closing the account or stop disbursal of remaining disbursal amount. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision.
- Where RE 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."

9. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

The Company shall undertake, that:

- Periodic Risk Assessment' exercise for 'Money Laundering (ML) and Terrorist Financing (TF);
- Risk assessment process should consider all the relevant risk factors, level of overall risk & type of mitigation to be applied;
- Risk assessment process shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company;
- Periodicity of risk assessment exercise shall be determined by the Board, which should be reviewed at least annually by the Internal Auditors of the company;
- Outcome of the exercise shall be put up to the Board/ Audit Committee;
- The risk assessment report/risk reporting matrix shall be put up to the Board annually and to the Risk Management Committee (RMC) meeting on a half yearly basis and quarterly by management.
- Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard;
- Monitoring of implementation of the controls and enhance them if necessary.

10. SANCTIONS LIST

The Company will comply with the various statutory/ regulatory requirements with regard to Sanctions List of individuals/ groups. In this regard, the Company will also comply with the order issued by the Government of India for implementation of Section 51-A of UAPA, 1967. Further, company shall also comply with instructions issued by Ministry of Finance, Government of India titled "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)". The Order stipulates detailed requirements and actions to be taken by the stakeholders for freezing / unfreezing of accounts, financial assets, etc., of individuals / entities designated under the list as specified under Section 12A of the WMD Act, 2005. The Company shall update list of such individuals/ entities from time to time based on the advice received from the Government/ Statutory/ Regulatory authorities.

The Company shall not enter into any transaction with a customer whose identity matches with any person with known criminal background or with banned entities and those reported to have links with terrorists or terrorist organizations identified by the Government/ Statutory/ Regulatory authorities. In case, any match is identified with any entity provided in the Sanctions List, the Company shall strictly follow the procedure required to be followed under the legal/ statutory/ regulatory requirements.

The Company shall also take the reference of updated published list of Financial Action Task Force (FATF) of the jurisdictions not fully /partly complying with the FATF Guidelines and ensuring that credentials of none of the existing /new customers matching with the details of persons/entity falling into non-compliance jurisdictions of FATF.

To ensure obligations under WMD Act, the Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

11. RISK MANAGEMENT THROUGH CATEGORISATION OF CUSTOMERS:

For the purpose of applying the RBI guidelines for identification and underwriting of potential customers, they will be broadly divided into low, medium and high-risk category. Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of employment, nature of business activity, and information about the customer's business, location of customer, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. The above-mentioned information when collected shall be non-intrusive in nature. While assessing the customer's identity, the Company may also factor in identity documents through online or other services offered by issuing authorities.

Basis the same, the categorization shall be as follows:

1. Low Risk:

a) People working at government departments, Public Sector Units, Public Limited companies, Multinational Companies etc;
b) Salaried employees whose salary structures are well defined and salary is paid by cheque / directly credited in the bank, including salaried applicants working with private companies or small enterprises where the income is verified with the employer;
c) Salaried employees whose salary structure is undefined and salary is paid in cash subject to cash salary being less than Rs. 30,000 (Thirty thousand only) monthly income.
d) All self-employed people under light-banking program
e) All self-employed professionals (Doctors, Chartered Accountant, etc.)
f) All self-employed non-professionals with no formal documents but with a sound business and earning less than equal to Rs. 75,000 (Seventy-five thousand only) assessed monthly income.

g) People belonging to lower economic strata of the society whose accounts show small balances and low turnover including but not limited to daily wage earner, person without permanent place of work, seasonal wage earners, contractual labour, milk seller, mechanic, small vendors, pan shop vendor will come under this category;

2. Medium Risk:

a) Salaried employees whose salary structure is undefined and salary is paid in cash subject to cash salary being more than Rs. 30,000 (Thirty thousand only) monthly income
b) Self-employed non-professional customers with no formal documents but with a sound business and earning more than Rs. 75,000 (Seventy-five thousand only) assessed monthly income

3. High Risk:

a) Politically Exposed Persons ("PEPS"), PEPs of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
b) Trusts, Charities, NGOs and organizations receiving donations;
c) High net worth individuals with income above 5 lakhs per month
d) Any individual with dubious reputation as per public information available;
e) Persons known to have been convicted of money laundering, drug trafficking, suspicious transactions or other serious crimes;
f) Non-Resident Indians (NRIs);

12. AML RISK:

The Company shall, inter alia, use the following tools to mitigate AML risk:

a) KYC documentation
b) Customer due diligence
c) Dedupe check
d) CIBIL Checks with credit scores
e) Reference checks
f) Tele verification
g) Field Investigation
h) Suspicious transaction reporting
i) Checking whether amount of loan is in line with disclosed sources of income and wealth

13. MONITORING RISK CATEGORISATION

A half yearly review shall be carried out of all the accounts / customers to determine the changes in risk categorization vis-a-vis the initial risk categorization as per the RBI guidelines provided from time- to-time w.r.t KYC policy.

Accounts/ Customers categorization shall be updated as per guidelines prescribed by RBI. The revised risk categorization shall be reviewed and approved by a committee of senior management. Since the loans given by the Company are long term in nature going up to 20 years, periodic review and updation of KYC shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers. However, if the Credit Head feel that a particular account / customer should be recategorized due to some extremely adverse circumstances, then he / she can recommend change in the risk categorization even before the prescribed timeline.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

The following guidelines shall be followed by the company regarding the risk management of the company:

a) The Company's internal audit department / engaged agency for internal audit, will evaluate and ensure adherence to the KYC policies and procedures. They will check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will also be put up before the Audit Committee of the Board as and when they meet. In addition to this, the Audit Committee will also ensure that the periodic evaluation of the Company's policies and procedures are done to ensure legal and regulatory compliance. The Company shall have an on-going employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focus for frontline/operations staff, compliance staff and staff dealing with new customers in order to make sure that the relevance and importance of this activity is understood by all employees irrespective of their functional roles;
b) The Company will educate the customer on the objectives of the KYC programme so that customer understands and appreciates the motive and purpose of collecting such information;
c) The Company will have adequate controls in place while deploying new technology / modifying existing technology to all threats that may arise due to loss of data / access to data which is critical;
d) In case a person who desires to open an account with the company is not able to produce the documents as required by CDD measures, the company may at its discretion can open an account subject to the conditions as defined in clause 24 and 39 of KYC directions of 2025, as given by RBI.

14. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain relevant documents to verify the applicant’s identity, place of residence, age etc. which are necessary to establish identity and contractibility of every new customer. The company will

ensure that all / any documents as listed in Annexure I are obtained from prospective customers in order to carry out the necessary due diligence for granting a loan.

The Company shall obtain satisfactory evidence of the identity of the customer in the following cases:

i. Commencement of an account-based relationship with the customer.
   If there are any perceived risks at the time of commencement of relationship/ opening of account, or there is a doubt about the authenticity or adequacy of the customer identification data it has obtained, or
ii. The Company shall also obtain relevant documents from an existing customer in case they change their place of residence. The evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.
iii. Company shall ensure that introduction is not to be sought while opening accounts.
iv. In order to avoid customer inconvenience, under special circumstances, the Company may also rely on certain data/information available with itself or with external reliable sources for the purpose of establishing the identity of the customer. In such cases, a KYC report in a specified format shall be prepared and approved by an appropriate senior official, as may be specified in the KYC/AML procedures. The KYC report shall be stored properly along with other KYC documents.
v. For opening of small value accounts, informal customer segment and smaller/ Semi- urban/ rural location, the Company may, at its discretion, apply differential procedures and provide relaxation in documentation and CDD requirements based on alternate verifications/ documents.
vi. The Company shall undertake offline verification of the proof of possession of the submitted documents where online verification is not permissible under the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025
vii. Appropriate Enhanced Due Diligence (EDD) measures shall be adopted for customers, with a high-risk profile, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs), resident outside India and their family members/close relatives.
viii. The EDD procedures should assist the Company in (a) determining whether the customer appears to be engaged in legitimate business activities and has legitimate sources of funds and (b) anticipating the customer's usual and expected activity so that suspicious activity can be detected

The Company's EDD procedures will consider requiring, at account opening stage that additional information and documentation be obtained on higher risk customers, for example, such as:

- Purpose of the account/ End-use.
- Source of funds and wealth.
- Banking references
- Citizenship or nationality for individuals
- Proximity of the customer's residence, place of employment, or place of business

- Description of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the business operations, the anticipated types, volumes and frequency of transactions, including currency and total sales, and a list of major customers and suppliers
- Explanations for changes in account activity

The Company's EDD procedures will consider requiring, periodically throughout the relationship that additional information and documentation be obtained on higher risk customers (who have moved from low risk to high risk), such as:

- Re-KYC in every 2 years.
- EDD is an ongoing process and the Company should take measures to ensure that information is current, and that appropriate risk-based monitoring occurs to ensure that any suspicious activity is escalated, analyzed, and reported, and that other appropriate action is taking

For all types of customers, the company will, either through its own officers or appointed agencies carry out verification of originals, place of residence etc. as well as take signature verification wherever necessary. In addition to this, the company's officers shall engage in a personal discussion with the customer/designated authority at his/her residence / place of work in order to interact with other family members/ workplace colleagues to evaluate the genuineness of the prospective customer.

15. ALLOTMENT OF UNIQUE CUSTOMER IDENTIFICATION CODE (UCIC)

As required by the RBI guidelines, the Company shall allot Unique Customer Identification Code to all its new customers while entering new relationships. The Company shall assign a unique loan id to every account and unique client id to every borrower and individual, who is part of the loan structure. Further for the existing customers such a code would be created within the permitted Companies Policy Guidelines on 'Know Your Customer' norms and Anti-Money Laundering measures timeframes. This UCIC will be used to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable company to have a better approach to risk profiling of customers.

16. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. It shall also exercise on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile. The CDD to be carried out is given in detail at Annexure 1.

The CDD, shall include:

- Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the

business relationship, where applicable;

- Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
- Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

The Company shall consider filing a suspicious transaction report, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk.

17. ONGOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce risk by having an understanding of the normal and reasonable activity of the customer so that it has the means of identifying transactions that fall outside the regular pattern of activity.
a) The Company will pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.
b) The extent of monitoring shall be aligned with the risk category of the customer. A system of periodic review of risk categorization of accounts, with such periodicity as specified in Company's KYC Policy shall be put in place.
d) Customers that are likely to pose a higher than average risk to the Company are categorized as medium or high risk. The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

18. PERIODIC UPDATION

Periodic KYC updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers.

The 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.

19. MONITORING OF TRANSACTIONS

On-going monitoring is an essential element of effective KYC procedures. Since, the Company is a housing finance company and all its loans are tenure based with a fixed instalment paid through electronic clearing system (ECS/NACH, DDM) mandate or post-dated cheques (PDCs), The Company's monitoring structure will be relevant to its nature of operations. While unusually large transactions will be rare given that the maximum loan the company currently offers is Rs. ₹50,00,000/- the company will still pay special attention to all unusually large cash transactions, disbursement or collections, relevant to its size of loans. Reporting for cash transactions especially for loan closures will be done and reviewed by the Management team periodically for identifying anomalies and to carry out due diligence if required as to source of funds or re-verifying identity of the borrower. Apart from this the Company will also carry out the following activities:

Risk categorization as is mentioned in this policy may be updated as and when required by the management;
In case of overdue / default accounts where there is scope for meeting or vetting the profile of this customer again, due diligence if found necessary will be carried out;
Subsequent to sanction, during the period of part disbursement, till full disbursement, if any unusual transaction / development comes to the Company's knowledge relating to money laundering the same will be verified and notified as required;
In addition, thereto, the Company will ensure that no disbursals are done in cash.

20. MAINTENANCE OF RECORDS OF TRANSACTIONS

Maintenance of Records of Transactions (As per Rule 3 of the Prevention of Money Laundering Rules 2005): The Company will maintain proper record of the under mentioned transactions:
All cash transactions of the value of more than Rupees ten lakhs or its equivalent in foreign currency or as required by latest regulations;
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 lakh or as required by latest regulations;
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 facilitating the transactions;
All suspicious transactions whether or not made in cash and as mentioned in Annexure II;
Records to contain the specified information: The records maintained shall contain the following:-

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.

d) the Parties to the transaction.

The Company shall ensure to implement a system/Software for maintaining transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The data and information of all existing sanction and disbursal files shall be uploaded on the software. This provides for a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required;

Maintain all necessary records of transactions between the company and the customer, both domestic and international, for at least five years from the date of transaction

The Company will ensure that records pertaining to the identification of the customer and his/her address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least 5 years after the business relationship is ended. Apart from this, the application form, copy of loan agreement, NOC, other document either photocopy or cancelled original copy will be kept for 5 years after the full closure of the account. Preservation and maintenance of the documents will be in paper form and also in digital form.;

The identification of records and transaction data will be made available to the competent authorities upon request only through the principal officer under this policy with his approval;

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

21. REPORTING TO FINANCIAL INTELLIGENCE UNIT (FIU-IND):

The Company will be reporting the information in the proper format, transactions relating to cash and suspicious nature to the Director, Financial Intelligence Unit-India (FIU-IND).
The information in respect of the transactions referred in rule 3 of the PML Rules is to be submitted to the Director every month by the 15th day of succeeding month.
Additionally, the Company will submit ‘Statement showing the details of Counterfeit Banknotes detected’ to the NHB within 7 days from the last day of the respective quarter.
Even in the case of ‘Nil’ instance also, the statement is to be submitted to the NHB.
The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by the Company, till installation /adoption of suitable technological tools for extracting CTR/STR from live transaction data.

The Company will monitor transactions to identify potentially suspicious activity. Such triggers will be investigated, and any suspicious activity to be submitted to the Director promptly, in writing or by E-mail, or by fax, not later than seven working days from the date of occurrence of such transaction and on being satisfied that the transaction is suspicious.

The Company will file the Suspicious Transaction Report (STR) to FIU -IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND. An illustrative list of Suspicious Transactions is enclosed as Annexure II of the Policy.

Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports - The Company will maintain utmost confidentiality in investigating suspicious activities and while reporting STR to the FIU-IND/ higher authorities. A Company Employee shall hold in strict confidence and not disclose to any third party a STR, information from or related to a STR, or the fact that a STR has been filed. Internally, only Employees with a need to know, such as investigators, attorneys involved in the investigation, Employees who must review and approve the STR, and auditors, can have access to STR related information.

Company shall not put any restriction on operations in the accounts where an STR has been filed and ensure that there is no tipping off by officials of the Company to the customer at any level. Officials keep the fact of furnishing of STR strictly confidential. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

22. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR):-

The Company will capture the KYC information/ details as per KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

1. 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. 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.

2. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
3. Where a Customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

    a. there is a change in the information of the Customer as existing in the records of CKYCR;
    b. the current address of the Customer is required to be verified;
    c. it is necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

23. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS):

The Company, if applicable, will adhere to the provisions of Income Tax Rules 114F, 114G, and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take requisite steps for complying with the reporting requirements in this regard.

24. COMPLIANCE WITH SECTION 51A OF UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967:-

The Company will ensure compliance with Section 51A of UAPA Act, 1987 by screening the prospective and existing account holders for UN Sanction List or any other list as per UAPA Act, 1987. In the event, any account holder resembles the name given in the list, it will be reported to FIU-IND and Ministry of Home Affairs. Further, other requirements including the freezing of assets, shall be followed by the Company.

25. HIRING & TRAINING OF EMPLOYEES AND CUSTOMER EDUCATION

Implementation of KYC Procedures requires the Company to seek information which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. To meet such situation, it is necessary that the customers are educated and apprised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company.

Employees: The Company shall put in place adequate screening mechanism as an integral part of employee recruitment/ hiring process. The Company shall train its employees (or the functions/groups) on KYC/ AML requirements/ procedures. The training requirements shall have different focus for frontline staff, compliance staff and staff dealing with new customers. The front

desk staff should be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML Measures policies of the Company, regulation and related issues should be ensured.

Customers: To educate the customers and win their confidence in this regard, the Company will arrange literature containing all the relevant information regarding KYC and AML measures. Such literature may be made available to the customers either directly or through the Company's website. Further, the Company staff will attend to the same promptly and explain reason for seeking any specific information and satisfy the customer in that regard.

26. AUDIT OF THE KYC & AML PROGRAM AND OTHER REPORTING REQUIREMENTS

To provide reasonable assurance that its AML Program is functioning effectively, an audit of its AML Program will be done as part of the internal audit of the Company. The audit will be conducted on a regular basis. The audit will include testing of the effectiveness of elements of the AML Program, compliance with applicable AML Laws, and the Company's related procedures.

The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

The books of accounts of persons authorised by Company including brokers/ DSAs or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

27. MISCELLANEOUS

The Company shall ensure that the provisions of PML, Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly along with any regulation or guidelines as prescribed by RBI or any other law. The persons authorized by the Company for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to the Company.

PART-1

ANNEXURE I: CDD for Individuals

While undertaking CDD, the company shall obtain the following information from an individual while establishing an account-based relationship with an 'individual' or dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:
a) the Aadhaar number where -
(i) s/he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) s/he decides to submit his Aadhaar number voluntarily to the company for authentication of AADHAR in terms of the first proviso to sub-section (1) of section 11A of the PML Act; or
(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and
(b) the Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time.
(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company
Provided that where the customer has submitted,
i) Aadhaar number above under clause (a) under first proviso to sub-section (1) of section 11A of the PML Act, company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by UIDAI. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information the Central Identities Data Repository, he may give a self-declaration to that effect to the Company.
ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, company shall carry out offline verification.
iii) an equivalent e-document of any OVD, company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified.
iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, company shall carry out verification through digital KYC as specified under this policy.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of company

and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection and shall be available for supervisory review.

Explanation 1: Where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, company shall ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.

ii. As regards borrower accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

iii. Borrower account, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out.

iv. If the CDD procedure as mentioned above is not completed within a year, no further debits shall be allowed.

v. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Regulated Entity. Further, while uploading KYC information to CKYCR, company shall clearly indicate that such accounts are opened using OTP based e-KYC and other Regulated Entities shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to- face mode.

vi. company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

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

i. The official performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information though Offline Verification of Aadhaar.

ii. A clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.

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

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

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

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

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

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

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

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

xi. company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp. Further the Company should also ensure that the entire data and recordings of VCIP shall be stored in a system located in India.

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

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

xiv. Business Correspondent/s (BC) can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence shall lie with company.

Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

Digital KYC Process

A. Develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application.

B. The access of the Application shall be controlled by company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given to authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official or vice-versa. The original OVD shall be in possession of the customer.

D. Ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer shall not be used for customer signature. Check that the mobile number used in customer signature shall not be the mobile number of the authorized officer must be ensured.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

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

List of Mandatory KYC Documents

List of KYC Documents for Individuals (anyone from the options available under the given category)	**Identity**	**Residence Address**	**DOB & Age Proof**
Voter ID	Yes	Yes	Yes
Passport	Yes	Yes	Yes
Driving License	Yes	Yes	Yes
Ration Card / BPL Card with Photo			Yes
PAN Card	Yes		Yes
Aadhar Card (redaction to be done on the physical Aadhar card number- first 8 digits)	Yes	Yes	Yes
Bills of Electricity/ Phone / GAS- Last 3 Months.		Yes	
NREGA Job Card	Yes		Yes
Birth Certificate			Yes
Education Certificate - Class 10^{th}& 12^{th}.			Yes
LIC Receipts & Bonds			Yes

Annexure-II: List of Suspicious Transactions Pertaining to Loan Accounts

1) Customer is reluctant to provide information, data, documents;
2) Submission of false documents, data, purpose of loan, details of accounts;
3) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc;
4) Reluctant to meet in person, represents through a third party / Power of Attorney holder without sufficient reasons;
5) Approaches a branch/office of the company, which is away from the customer's residential or business address provided in the loan application, when there is Company branch/office nearer to the given address;
6) Initial contribution made through unrelated third-party accounts without proper justification;
7) Availing a top-up loan and / or equity loan, without proper justification of the end use of the loan amount;
8) Suggesting dubious means for the sanction of loan;
9) Where transactions do not make economic sense;
10) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
11) Encashment of loan amount by opening a fictitious bank account;
12) Applying for a loan knowing fully well that the property / dwelling unit to be financed has been funded earlier and that the same is outstanding;
13) Sale consideration stated in the agreement for sale is abnormally higher / lower than what is prevailing in the area of purchase;
14) Multiple funding of the same property / dwelling unit;
15) Usage of loan amount by the customer in connivance with the vendor / builder / developer / broker / agent etc. and using the same for a purpose other than what has been stipulated;
16) Multiple funding / financing involving NGO / Charitable Organization / Small / Medium
17) Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs);
18) Frequent requests for change of address;
19) Overpayment of instalments with a request to refund the overpaid amount
20) A customer who suddenly starts making payments in multiple instalments when it is known that the customer does not have the capacity to do so.
21) Bank transactions that cannot be matched with the income levels of the customer.
22) A client whose bank statement indicates large or frequent deposits and sums are immediately withdrawn.
23) customers whose deposits contain counterfeit notes or forged instruments;
24) customers who repay problem loans unexpectedly;

PART-II

ANNEXURE 3 - Enhanced Due Diligence ("EDD") Measures

The Company shall apply enhanced due diligence measures for higher risk customers i.e. Customers that are likely to pose a higher-than-average risk to the Company, especially those for whom the sources of funds are not clear. Such category of customers will include the following:

- Non face to face customers
- Any individual with dubious reputation as per public information available
- Politically Exposed Persons (PEP's),
- Non-Resident Indians,
- Certain Non-Governmental Organizations ("NGOs"), Trusts and unregulated charities,
- Money services businesses ("MSBs"), including licensed money transmitters and currency exchangers, and their owners,
- Antique dealers and auction houses, and their owners,
- Casinos and other gambling businesses, their payment providers, and their owners,
- Customers organized, doing business in, or that maintain financial accounts in, jurisdictions that pose a high risk of/are convicted of money laundering, drug trafficking, terrorism, terrorist financing, or corruption or jurisdictions that are not logical for the customer,

- In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall be adopted.
- The Company shall 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, etc. For this purpose, the Company shall maintain lists of individuals or entities issued by Reserve Bank, National Housing Bank, United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/entities in the list shall be treated as suspicious and reported.
- The Company shall not open an account where it is unable to apply appropriate customer due diligence measures i.e., it is unable to verify the identity and /or obtain documents required due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company.
- 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 may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision.

Under the Company's EDD procedures, at account opening stage that additional information and documentation be obtained on higher risk customers, for example, such as:

- Purpose of the account/ End-use.
- Source of funds and wealth.

- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors.
- Financial statements
- Banking references
- Domicile (where the business is organized)
- Citizenship or nationality for individuals
- Proximity of the customer's residence, place of employment, or place of business
- Description of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the business operations, the anticipated types, volumes and frequency of transactions, including currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activity

In terms of extant regulatory guidelines, the Company will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. The Company's EDD procedures will consider requiring, periodically throughout the relationship that additional information and documentation be obtained on higher risk customers (who have moved from low risk to high risk). The Company will carry such review of risk categorization of customers 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 will not be less than once in five years in case of low-risk category customers and not less than once in two years in case of high risk categories.

EDD is an ongoing process and the Company should take measures to ensure that information is current, and that appropriate risk-based monitoring occurs to ensure that any suspicious activity is escalated, analyzed, and reported, and that other appropriate action is taking.

PART-3

ANNEXURE IV: Customer’s Accounts Opened By Professional Intermediaries

The Company shall ensure while opening customer's accounts through professional intermediaries, that:

a) Customer shall be identified when client account is opened by a professional intermediary on behalf of a single client.

b) The Company shall have an option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

c) The Company will not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the Company, the Company will look for the beneficial owners.

e) The Company will, at discretion, rely on the CDD done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

It should be understood that the ultimate responsibility for knowing the customer vests with the HFC.