
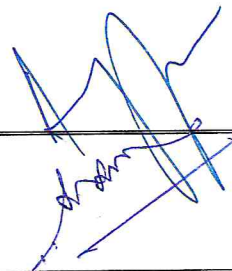

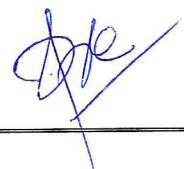




KYC & AML POLICY-3.0

MAY 2021

1Particulars	Name	Designation	Signature
Recommended by	Indranath Bose	HPPR	
	Anurag Jain	CCCO	
Approved by	Sunil Gupta	CEO	
	Deepak Joshi	Vice Chairman & Director	
	Meghha Gupta	Chairman & Managing Director	

KYC & AML Policy

1. Introduction:

Manibhavnam Home Finance India Pvt Limited (hereinafter referred to as "the Company" or "HFC" or "Lender" or "MBHF" or "Manibhavnam" or "Regulated Entity/ RE") is a Private Limited Company incorporated under the provisions of the Companies Act, 2013 and registered as a Housing Finance Company ("HFC") with the National Housing Bank ("NHB").

With the shifting of regulation of HFCs from NHB to RBI, now Reserve Bank of India ("RBI") vide their circular (RBI/2019-20/235 DOR.NBFC (HFC). CC. No.111/03.10.136/2019-20) dated May 19, 2020 made Master Direction - Know Your Customer (KYC) Direction, 2016, applicable to all HFCs. Subsequently, RBI vide circular dated February 17, 2021(RBI/2020-21/73, DOR.FIN.HFC.CC. No.120/03.10.136/2020-21) re-iterated the applicability of the above Master Direction - Know Your Customer (KYC) Direction, 2016. Manibhavnam Home Finance India Pvt Ltd (MBHF) has adhered to the guide lines towards KYC/AML policy.

2. OBJECTIVES:

The present policy is designed with an objective to evolve the monitoring and reporting system as prescribed in the above said RBI's Master Directions and other relevant regulations to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions

3. SCOPE:

3.1 Applicability

The Know Your Customer and Anti-Money Laundering Policy (the Policy) shall be applicable to Manibhavnam as notified by the RBI from time to time. The Policy framed thereunder and approved by the Board shall also apply to any third parties relied upon or hired by the Company to perform any of the requirements relating to KYC & Anti-Money Laundering (AML) Program.

This Policy establishes minimum requirements for the Company to establish, implement, and maintain an AML Program that is reasonably designed to (a) implement this Policy and (b) to ensure compliance with applicable AML laws, rules and regulations.

This Policy requires the Company and each Employee to:

- Protect the Company from being used for money laundering or funding terrorist activities;
- Conduct themselves in accordance with the highest ethical standards
- Comply with the letter and the spirit of applicable AML Laws, and the Company's AML Program and procedures;



2



- Be vigilant and escalate AML procedures in respect of individuals/entities who attempt to violate or avoid KYC /AML, procedures or this Policy; and
- Cooperate with AML-related law enforcement and regulatory agencies fully under applicable laws.
- Designate official for reporting purposes to Financial Intelligence Unit (FIU).

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 businesses' policies and procedures.

3.2 Annual Review

The Policy shall be reviewed annually by the Board of Directors of the Company, the Principal Officer and, more frequently, if the changes are required due to modifications in applicable directions, rules and regulations.

3.3 Implementation & Monitoring of Policy

The Audit Committee (AC) shall supervise the implementation and monitoring of the Policy. Amongst other matters, the AC would be responsible for:

- Formulating and periodically reviewing the Policy in line with the applicable regulatory guidelines;
- Reviewing the reports submitted by the Principal Officer (PO)/ the Money Laundering reporting Officer (MLRO) from time to time;
- Instituting an KYC/AML training program;
- Establishing appropriate internal controls, procedures and systems in regard to fraud prevention, KYC/AML etc.

3.4 Policy Approval

The Policy and any significant changes therein shall be approved by the Board of Directors of the Company. Prior to approval by the Board of Directors, the Policy and any significant changes shall also be reviewed by the Audit Committee of the Board, taking into account the feedback of Company's Principal Officer and also based on internal audit report on implementation of KYC and AML procedures which have been brought under the scope of internal audit.

4. POLICY STANDARDS AND AML PROGRAM STRUCTURE

4.1 The KYC and AML Policy has been prepared considering the following 4 key elements:

- Customer Acceptance Policy (CAP)
- Customer identification Procedures (CIP)
- Monitoring of Transactions, and
- Risk Categorization

The bottom of the page features three handwritten signatures or initials. The first is a large, stylized signature. The second is a signature that appears to be 'DZ'. The third is a signature that appears to be 'S NG'.

4.2 For the purpose of the Policy, a 'Customer' is defined as:

- a person or entity (including an employee) that maintains an account and/or has a business relationship with the Company.
- one on whose behalf the account is maintained (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, say, a wire transfer or issue of a high value demand draft as a single transaction.

4.3 Beneficial Owner (BO)

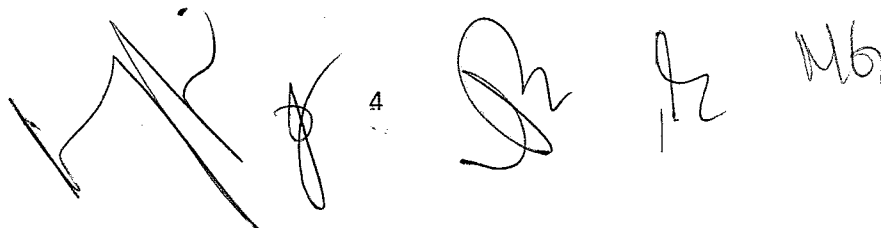
- Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

- "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
- "Control" shall include the 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 shareholders agreements or voting agreements.
- Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.
- Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

- Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.



Handwritten signatures and initials, including a large signature on the left, a small signature in the middle, and several initials on the right, including 'Mb'.

4.4 Certified Copy- Obtaining a certified copy by the Company 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 authorised officer of the Company as per the provisions contained in the Act.

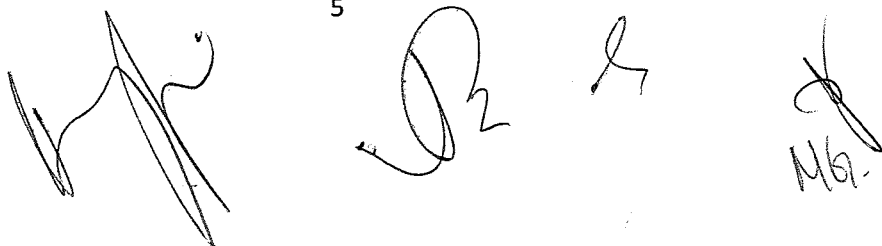
4.5 The Company is aware that availability of sufficient customer information underpins all other AML procedures and should be seen as a critical element in the effective management of Money Laundering (ML) risks

4.6 Customer Acceptance Policy (CAP)

The Company has evolved a Customer Acceptance Policy (CAP) which lays down the criteria for the acceptance of Customers. In line with the RBI's Master Direction - Know Your Customer (KYC) Direction, 2016, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers which forms an integral part of the Group AML Policy.

The features of the CAP are detailed below:

- The Company shall not open any account(s) in anonymous, fictitious or 'benami' name(s). Adequate customer due diligence (CDD) is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate basic due diligence.
- The nature and extent of basic due diligence measures to be conducted at the time of establishment of account opening/relationship, would depend upon the risk category of the customers and involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the ML risks posed by the applicant and the applicant's expected use of The Company's products and services.
- If allowed by the regulations, the Company may rely upon the KYC procedures conducted by other Banks/ Intermediaries having satisfactory customer identification procedures.
- For non-face to face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such

The page contains four handwritten signatures or initials. From left to right: a large, stylized signature; a signature that appears to be 'R2'; a small, simple signature; and a signature that appears to be 'MG'.

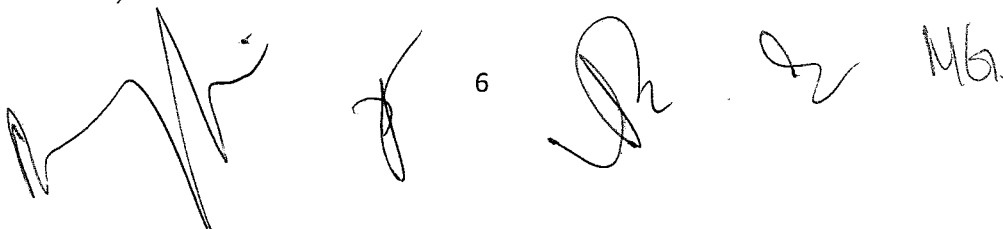
customers. With regard to cross border customers, Company may rely on third party certification/introduction. In such cases it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

- The purpose of commencing the relationship/opening of accounts shall be established and the beneficiary of the relationship/account shall also be identified.
- The information collected from the customer shall be kept confidential.
- 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.
- 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.

The aspects mentioned in the CAP would be reckoned while evolving the KYC/AML procedures for various customers/products. However, while developing the KYC/CDD procedures, the Company shall ensure that its procedures do not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society.

4.7 Customer Identification Procedures

- The Company shall obtain satisfactory evidence of the identity of the customer in the following cases:
 - If there is any perceived risks at the time of commencement of relationship/opening of account, or



Handwritten signatures and initials, including a large signature on the left, a small signature in the middle, and the initials 'MB' on the right.

- when there is a doubt about the authenticity or adequacy of the customer identification data it has obtained, or
 - selling third party products as corporate agents, selling own products and any other product for more than rupees fifty thousand, or
 - when there is a reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.

- Company shall ensure that introduction is not to be sought while opening accounts.
- 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.
- 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.
- Indicative guidelines on Customer Identification requirements are provided in the Annexure 1.

4.8 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;
- Outcome of the exercise shall be put up to the Board/ Audit Committee;
- 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.

4.9 Risk Categorization

Low Risk: For the purpose of risk categorization individual and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known

profile, shall be categorized as low risk. Given our focus and policy outlining all of our customers will fall in low-risk category. Illustrative examples of low-risk customers are –

- All Salaried customers whose salary structures are well defined
- People belonging to government department, PSU, Public & private limited and multinational companies.
- Self-employed customers with proper income documents such as ITR, P&L, Balance Sheet and current account etc.
- People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
- Self-employed people with sound business & profitable track record for a reasonable period where we can verify with suppliers / customers as to nature and volume of business transactions as well as credibility in business dealings.

Medium Risk: The medium risk customers shall be categorized on the basis of the customer's background, nature and location of activity, country of origin, sources of funds and client profile. Medium Risk customers shall include

- high net worth individuals,
- companies having closed family shareholding or beneficial ownership

High Risk: Individual or entities that pose a higher-than-average risk to the company will be categorized as high-risk customers. This will be ascertained at the time of credit underwriting after looking at the customer's background, nature of business, employment, predictability of cash flows etc. Illustrative examples of high-risk customers are -

- Non-resident customers,
- Trusts, charities, NGOs and organizations receiving donations,
- Firms with 'sleeping partners',
- Politically exposed persons (PEPs) of foreign origin,
- Non-face to face customers, and
- Those with dubious reputation as per public information available, etc.

Adoption of Customer Acceptance Policy and its implementation will not result in denial of MBHF's services to the general public, especially to those who are financially or socially disadvantaged. Our exposure to any of our customers is subject to our credit risk policy and operations manual. However, for customer acceptance, KYC is a prerequisite for a credit risk grading.

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

- KYC documentation
- Customer due diligence
- Dedupe check
- Bureau Checks with credit scores
- Reference checks

MG.

- Tele verification
- Field Investigation
- Limit on amount of loan in cash
- Suspicious transaction reporting
- Checking whether amount of jewelry or loan is in line with disclosed sources of income and wealth

4.11 KYC and Customer Due Diligence (CDD)

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.

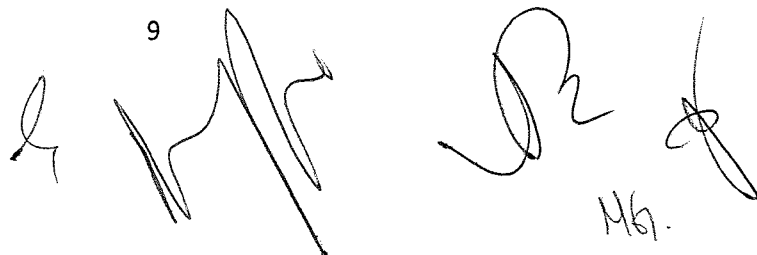
For undertaking CDD, following should be obtained from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

- the Aadhaar number where, (i) 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 he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or the proof of possession of Aadhaar number where offline verification can be carried out; or 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
- the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority; and
- 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:

Provided that where the customer has submitted,

- Aadhaar number, authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect.
- proof of possession of Aadhaar where offline verification can be carried out, the same shall be done.
- an equivalent e-document of any OVD, then, shall verify the digital signature as prescribed.

9



The image shows four handwritten signatures or initials in black ink. The first is a simple 'L' shape. The second is a stylized, elongated signature. The third is a circular, scribbled signature. The fourth is a signature with the initials 'MG.' written below it.

- any OVD or proof of possession of Aadhaar number, where offline verification cannot be carried out, verification to be carried out through digital KYC process as prescribed.

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, 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.

Note 1: where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required.

Note 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Note 3: 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 and as amended from time to time.

Note 4: REs other than banks can only carry out Offline Verification of Aadhaar for identification.

Note 5: For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his/her identity shall be undertaken keeping in view the following:

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

5. Enhanced Due Diligence ("EDD")

The Company will include reasonable risk based EDD procedures for its higher risk customers.

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. Higher-risk customers must be approved by Chief of Credit , Collection & Operation and the customer's transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship.

Handwritten signatures and initials at the bottom of the page, including a signature with the number '10' and initials 'Sh 146'.

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.
- 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 :

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:

- Updation of KYC documents 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.

6. Politically Exposed Persons ("PEPs")

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Company shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

7. Negative List

The branches of Manibhavnam shall maintain a local negative list of persons, to the extent it is possible, and after a thorough name check of the client base by the respective branches, it will ascertain if there is any such match. In the event of a match against one of the local negative lists that is of credit related nature only (no other negativities associated with the name), the PO/ MLRO or any other person with appropriate authority shall have the discretion to approve acceptance of the client/prospect.

11

The image shows several handwritten signatures and initials in black ink. On the left, there is a small, stylized signature. In the center, there is a larger, more complex signature with the number '11' written above it. To the right of this, there are two more signatures: one that appears to be 'R2' and another that is less legible but includes the letters 'MB'.

8. Sanctions List

Manibhavnam will comply with the various statutory/ regulatory requirements with regard to Sanctions List of individuals/ groups. In this regard, Manibhavnam will also comply with the order issued by the Government of India for implementation of Section 51-A of UAPA, 1967. 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.

9. APPOINTMENT OF THE PRINCIPAL OFFICER (PO) / MONEY LAUNDERING REPORTING OFFICER (MLRO) & DESIGNATED DIRECTOR.

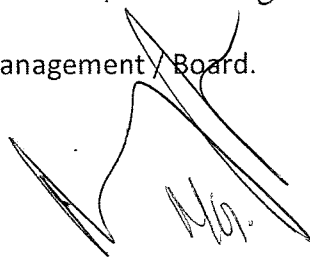
A senior official of the Company shall be designated as the Principal Officer of the Company. The Principal Officer shall be responsible for overseeing and managing the AML Implementation ensuring the compliance of the Regulatory Directions. The Principal Officer shall be responsible for the day-to-day functioning of the Company's AML Implementation and must have the knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business.

Also, the MD of the company shall also be the Designated Director for reporting purposes and the same shall be communicated to the FIU or other regulatory institutions.

Explanation: The term "Senior Official" mean and include an official of the Company not below the rank of H.O.D or immediately below the level of MD or CEO.

Key Responsibilities of the Principal Officer (PO)/ MLRO

- The PO must be able to assist the respective business heads to assess the ways in which products (existing or under development) may be abused by money launderers.
- The PO must be capable of assisting the respective business heads to evaluate whether any activity is suspicious under the Manibhavnam 's standard and under any applicable local law.
- Monitoring the implementation of the company's KYC/AML policy.
- Reporting of transactions and sharing of the information as required under the law.
- Maintaining liaison with regulatory authorities.
- Ensuring submission of periodical reports to the top Management / Board.



- Organizing continual training of employees to make them aware and keep them up to date with requirements of PMLA and any amendments thereto.
- Review all reports required to be submitted to regulatory/law enforcement authorities
- Reporting to the FIU-IND
- Monitoring of compliance and exception reporting.

Key Responsibilities of the Designated Director

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

10. REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA

Section 12 of PMLA requires every housing finance company to report information of transaction referred to in clause (a) of sub-section (1) of Section 12 read with Rule 3 of the PML Rules relating to cash and suspicious transactions etc. to the Director, Financial Intelligence Unit-India (FIU-IND). Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

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 Principal Officers shall make suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website "<http://fiuindia.gov.in>".

Principal Officer shall ensure there is no delay in reporting a transaction as delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation.

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.

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.

The bottom of the page features four distinct handwritten signatures or initials. From left to right: a stylized signature, a signature that appears to be 'D2', a signature that looks like 'M', and a signature that includes the letters 'MB'.

11. Reporting of Cash Transactions

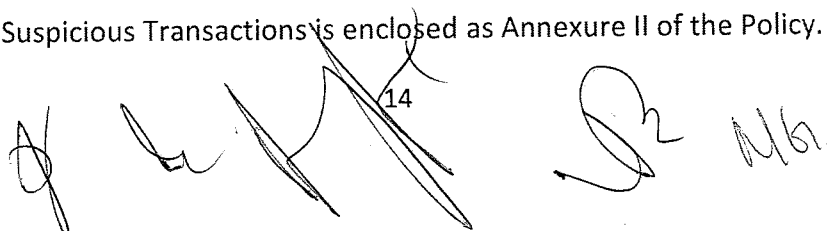
- Cash Transaction Report- In accordance with the requirements under PMLA, the Company will file Cash Transaction Report (CTR) for each month to FIU -IND by 15 days of the succeeding month. CTR should include the following:
 - all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
 - all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh 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
- Counterfeit Currency Report - In addition to the above, all cash transactions, where forged or counterfeit Indian currency notes have been used as genuine will also be reported by the Company to FIU-IND as Counterfeit Currency Report (CCR) not later than seven working days from the date of occurrence of such transactions. These cash transactions should also include transactions where forgery of valuable security or documents has taken place.
- According to the revised Master Directions, effective from February 17, 2021, the company shall ensure to furnish a quarterly report to the NHB along the lines of Annexure-VI (copy enclosed) of the Reserve Bank of India (RBI) Master Circular-Detection and Impounding of Counterfeit Notes dated July 01, 2020, as amended from time to time, and similar instructions issued by the Bank. The above report should be furnished to the NHB within 7 days of the end of the quarter. A "nil" report should be sent in case no counterfeit has been detected during the quarter. (Refer to instructions under para 108.2 Chapter XIV – Miscellaneous instructions of the Master Directions.)

12. Suspicious Transactions Monitoring and Reporting-

In accordance with suspicious transactions monitoring and reporting laws the Company will establish risk-based procedures and manual processes or automated systems, for monitoring transactions to identify, investigate, and escalate potentially suspicious activity; report suspicious activity to appropriate government authorities, and take other appropriate action, such as terminating a customer relationship. The Company's Principal Officer is charged with the responsibility of coordinating and overseeing suspicious activity monitoring, including making reports to the FIU -IND.

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.

Handwritten signatures and initials, including the number 14, are present at the bottom of the page.

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.

The Company will ensure that the customer is not tipped off on the STRs made by them to FIU- IND.

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.

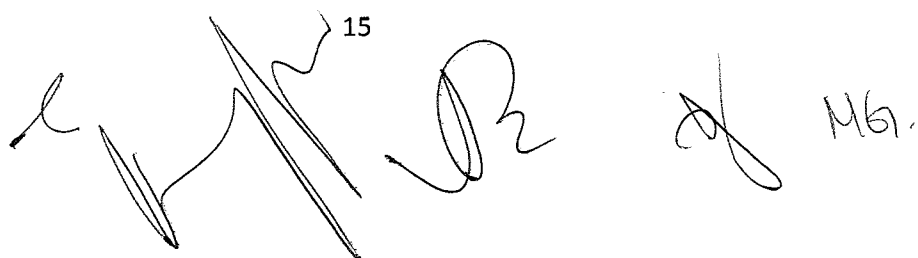
13. RECORDKEEPING REQUIREMENTS

13.1 The Company shall introduce a system of maintaining proper record of transactions as required with reference to provisions of PML Act and Rules, as mentioned below:

- To 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;
- To make available the identification records and transaction data to the competent authorities upon request;
- To introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.
- all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh 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;
- all transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions; and
- all suspicious transactions whether or not made in cash and by way of as mentioned in the Rule 3(1) (D).
- records of the identity of all clients of the Company shall be maintained for a period of eight years from the date of cessation of transactions between the clients and the Company.

13.2 Records to contain the specified information- The above records, in terms with Rule 3 of the PMLA Rules, to contain the following information:

15

The image shows several handwritten signatures and initials in black ink. From left to right, there is a signature that appears to be 'e', a large stylized signature, a signature that looks like 'R', and a signature that looks like 'M.G.'.

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

13.3 The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

14. 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 HFC, 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.

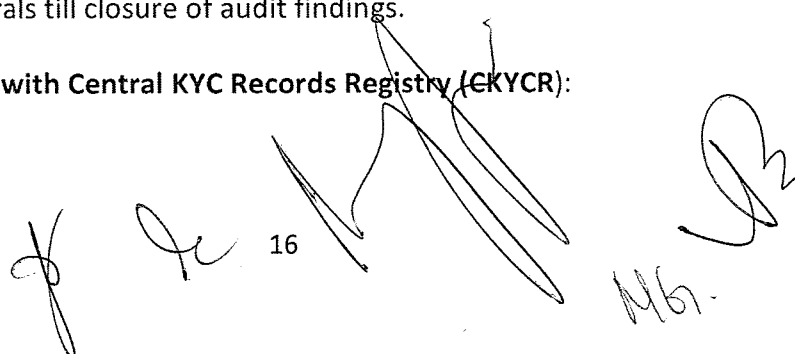
15. AUDIT OF THE KYC & AML PROGRAM AND OTHER REPORTING REQUIREMENTS

To provide reasonable assurance that its KYC & AML Program is functioning effectively, an audit of its KYC & 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 KYC & AML Program, compliance with applicable KYC & 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 or half yearly intervals till closure of audit findings.

16. Sharing KYC information with Central KYC Records Registry (CKYCR):

16



The bottom of the page features several handwritten signatures and initials. On the left, there are two distinct signatures. In the center, there is a large, stylized signature. To the right of this, there are initials 'MB.' and another signature that appears to be 'B2'.

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.

17. 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 as per the following procedure:

MBHF shall carry out:

- PAN verification from the verification facility available with the issuing authority and
- Authentication, of Aadhaar Number already available with the MBHF with the explicit consent of the customer in applicable cases.
- In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
- Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorised as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.
- In case of Legal entities, MBHF shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- MBHF may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD / Consent forwarded by the customer through mail/ post, etc., shall be acceptable.
- MBHF shall ensure to provide acknowledgment with date of having performed KYC updation.
- The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

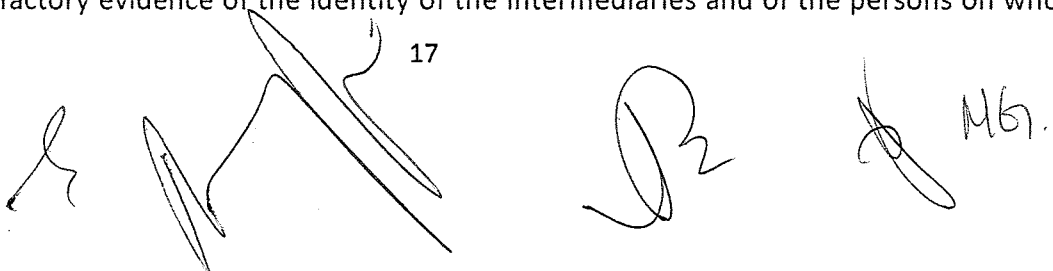
Annexure I

A. CUSTOMER IDENTIFICATION MINIMUM REQUIREMENTS- INDICATIVE GUIDELINES

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The Company will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, The Company will insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose

17

The image shows several handwritten signatures and initials. On the left, there are three distinct signatures. In the center, there is a large, stylized signature with the number '17' written above it. To the right of this, there are two more signatures, one of which appears to be 'MBF'.

behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, The Company will take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

For opening an account of a trust, one certified copy of each of the following documents or the equivalent e-documents shall be obtained:

- Registration certificate;
- Trust deed;
- Permanent Account Number or Form No.60 of the trust;
- one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Numbers of Form 60 of the beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

Accounts of companies and firms

The Company will be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks or REs. The Company will examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

For opening an account of a company/ firm, one certified copy of each of the following documents or the equivalent e-documents shall be obtained:

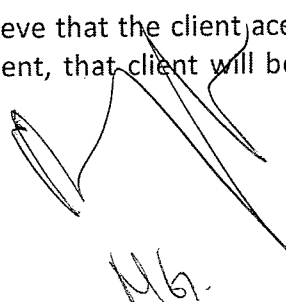
- Certificate of incorporation/ Registration Certificate;
- Memorandum and Articles of Association / Partnership deed;
- Permanent Account Number of the company/ firm;
- A resolution from the Board of Directors and/ or power of attorney granted to its managers, officers, Partner or employees to transact on its behalf;
- one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Numbers of Form 60 of the beneficial owner, the managers, officers, Partners or employees, as the case may be, holding an attorney to transact on the company's/ Partnership behalf.

Client accounts opened by professional intermediaries

When the Company has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client will be identified as per procedure listed above or as per this policy.



18



167.



Accounts of Politically Exposed Persons(PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Company will gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. The Company will verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP will be taken by CCCO level or above. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Accounts of non-face-to-face customers

In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there will be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented will be insisted upon and, if necessary, additional documents will be called for as deems required by the Company for effective CDD and Identification per applicable RBI directions or PMLA or Rules made thereunder.

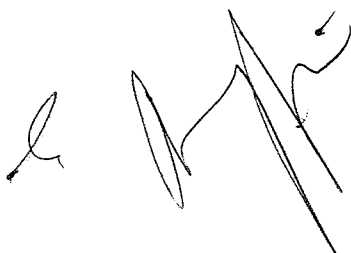
B. INDICATIVE LIST OF THE NATURE AND TYPE OF DOCUMENTS/ INFORMATION

For purpose of this policy "Officially Valid Document" (OVD) shall means:

- Passport;
- Driving License;
- Proof of Possession of Aadhaar Number;
- 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;
- Letter issued by the National Population Register containing details of name and address;

Provided that:

- 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;
- 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 pension 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;
- the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

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.

A. KYC DOCUMENTS LIST:

These are to be taken individually for all applicant, co applicant and guarantor if applicable

<p>Identity proof</p>	<ul style="list-style-type: none"> ✓ Pan Card ✓ Valid Passport ✓ Voter ID Card ✓ Valid Driving License ✓ Aadhar Card ✓ Employee ID Card of a listed organization Government Photo ID Cards / Service photo identity card issued by PSU ✓ Ration card with Photo pasted and stamped ✓ Notarized Affidavit in absence of any of the above documents (Original)
<p>Residence Address Proof</p>	<ul style="list-style-type: none"> ✓ Valid Passport ✓ Voter ID Card ✓ Valid Driving License ✓ Aadhar Card ✓ Bank Statement or Pass Book having mention of address – Not older than 2 months ✓ Property Tax receipt not more than 2 months' old ✓ Electricity bill – not older than 2 months ✓ Landline Telephone Bill – not older than 2 months ✓ Any Utility bill (Electricity, Water, Phone, Mobile, Internet, PNG Gas, Gas Cylinder delivery receipt) – not older than 2 months ✓ Credit Card Statement – not older than 2 months ✓ Life Insurance Premium Paid Receipt - Not more than 2 months' old

Handwritten signatures and initials are present at the bottom of the page, including a large signature on the left, the number '20' in the center, and several other initials and scribbles on the right side.

	<ul style="list-style-type: none"> ✓ Ration Card in the name of the individual or immediate family with relationship mentioned or address proof attached ✓ Letter from UIDAI containing name, address and Aadhar No. ✓ PAN Intimation letter along with PAN Card (having Same PAN no. as provided) ✓ Any document or communication issued by any authority of the central Government, State Government or local bodies showing residential address ✓ Notarised or Registered Rent agreement / leave & license agreement in the name of applicant ✓ Any property document supported by Positive FI ✓ Notarized Affidavit in absence of any of the standardized document (Original) ✓ Any valid document of spouse / parents supported by valid relationship proof
Date of Birth proof	<ul style="list-style-type: none"> ✓ Pan Card ✓ Valid Passport ✓ Valid Driving License ✓ School leaving certificate / 10th Pass Certificate ✓ Birth Certificate ✓ Any document or communication issued by any authority of the Central Govt., State Govt., or Local Bodies showing Date of Birth ✓ Notarized Affidavit in absence of any of the above documents (Original)
Signature Proof	<ul style="list-style-type: none"> ✓ Pan Card ✓ Valid Passport ✓ Valid Driving License ✓ Banker Verified Signature Verification ✓ Processing Fees Cheque clearance

B. Digital KYC Process

For the purpose of this section:

“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

Handwritten signatures and initials, including a large stylized signature with '21' written above it, and another signature that appears to be 'R' followed by 'M.G.'.

longitude of the location where such live photo is being taken by an authorised officer of our company as per the provisions contained in the Act.

“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.

“Video based Customer Identification Process (V-CIP)”: a method of customer identification by an official of the 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 Policy.

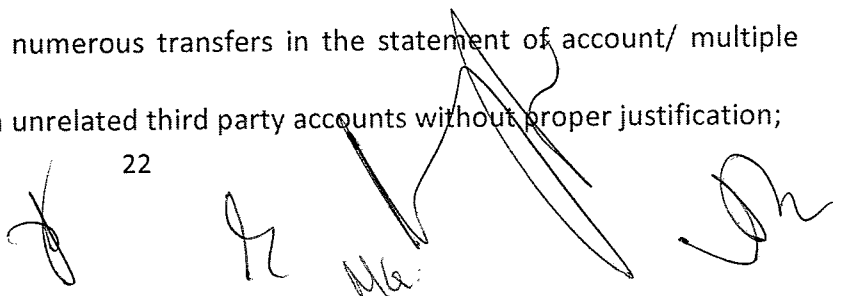
In case a customer apply for digital KYC process then:

- The original OVD is required to be presented.
- Live photograph of the customer shall be taken and the same photograph is embedded in the Customer Application Form (CAF).
- Other guidelines as per the directions of RBI are followed while capturing the Photograph and OVD documents.
- OTP validation, shall be carried out for successful signing of authorized officer on the declaration.
- Thereafter, the Application shall give information about the completion of the process and submission of activation request and also generate the transaction-id/reference-id number of the process. Transaction-id/reference-id shall be intimated to the customer for future reference. Verification shall be done by our officer and CAF shall be digitally signed.

Annexure II

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO HOUSING LOANS:


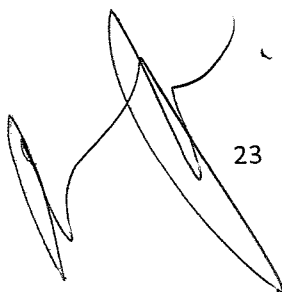
- Customer is reluctant to provide information, data, documents;
- Submission of false documents, data, purpose of loan, details of accounts;
- Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
- Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
- Approaches a branch/office of a HFC, which is away from the customer’s residential or business address provided in the loan application, when there is HFC branch/office nearer to the given address;
- Unable to explain or satisfy the numerous transfers in the statement of account/ multiple accounts;
- Initial contribution made through unrelated third party accounts without proper justification;

Handwritten signatures and initials are present at the bottom of the page. From left to right, there is a signature that appears to be 'J', followed by the initials 'R', then 'M.G.', and finally a large, stylized signature that looks like 'S.R.'.


- Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
- Suggesting dubious means for the sanction of loan;
- Where transactions do not make economic sense;
- There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
- Encashment of loan amount by opening a fictitious bank account;
- 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;
- Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
- Multiple funding of the same property/dwelling unit;
- Request for payment made in favour of a third party who has no relation to the transaction;
- 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.
- Multiple funding / financing involving NGO / Charitable Organisation / Small / Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs)
- Frequent requests for change of address;
- Overpayment of instalments with a request to refund the overpaid amount

II. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER/PROJECT LOANS:

- Builder approaching the HFC for a small loan compared to the total cost of the project;
- Builder is unable to explain the sources of funding for the project;
- Approvals/sanctions from various authorities are proved to be fake;

  23



 M6.