



Know Your Customer (KYC) – Anti-Money Laundering (AML) Policy

April 2024

Ver. 6.0

Know Your Customer and Anti-Money Laundering Policy

Version	Date
1.0	June 15, 2010
2.0	April 1, 2013
3.0	January 1, 2017
4.0	April 1, 2020
5.0	April 1, 2021
6.0	April 1, 2024

1. Background:

The Company (i.e. "Svatantra Micro Housing Finance Corporation Limited"/ "SMHFC"/ "RE") has in place Know Your Customer and Anti-Money Laundering Policy (KYC-AML Policy/The Policy) which was approved by the Board of Directors in the meeting dated June 15, 2010.

Reserve Bank of India (RBI) vide its press release dated August 13, 2019, on Transfer of Regulation of HFCs to RBI, advised that Housing Finance Companies (HFCs) will be treated as one of the categories of Non-Banking Financial Companies (NBFCs) for regulatory purposes and RBI will carry out a review of the extant regulatory framework applicable to the HFCs and come out with revised regulations in due course.

RBI has since advised extending the Master Direction- Know Your Customer (KYC) Direction, 2016 to Housing Finance Companies vide its Circular DOR.NBFC (HFC).CC No.111/03.10.136/2019-20 dated May 19, 2020. Hence, the RBI Master Direction – Know Your Customer (KYC) Direction, 2016 Ref. No. DBR.AML.BC. No.81/14.01.001/2015-16 dated February 25, 2016, updated from time to time and last updated on January 04, 2024, are now applicable to Housing Finance Companies and the instructions/ guidelines/ regulations contained in the circulars issued by National Housing Bank stands repealed.

In view of the above, the existing Policy has been reviewed by incorporating the latest RBI guidelines and provisions of the PML Rules and Act.

2. Objective of the Policy:

The KYC-AML policy shall include the following four elements:

1. Customer Acceptance Policy;
2. Risk Management;
3. Customer Identification Procedures (CIP); and
4. Monitoring of Transactions.

The key objective of the Policy is to ensure that the Company's money is not used intentionally or unintentionally, directly or indirectly, for any unlawful and prohibited activities or purpose particularly those which are covered by Prevention of Money Laundering Act, 2002 (PMLA). At the same time the Policy will also enable the Company to have more transparent and specific information about their customers and their financial dealings which will enable the Company to effectively determine risk level involved in different Loan transactions and will help the Company to undertake effective risk management.

SMHFC's KYC-AML Policy is applicable to all types of customers including individuals, partnership firms, employees, corporate entities, associations, trusts, societies and juridical persons. This policy also covers the Natural and Juridical persons who are the ultimate beneficiaries of the credit facilities extended by the Company and the natural persons who represent such persons or entities. The policy is also applicable to the persons authorized by SMHFC including brokers/ agents etc.

3. Definitions:

In this policy, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them under the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

Sr. No	Term	Definitions
1	Aadhaar Number	Identification Number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act'.
2	Act and Rules	The Prevention of Money-Laundering Act, 2002 ("Act") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, ("Rules") and amendments thereto.
3	Authentication	Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
4	Beneficial Owner (BO)	<p>(i) 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 person, has/have a controlling ownership interest or who exercise control through other means.</p> <p>Explanation - For the purpose of this sub-clause: -</p> <p>a) Controlling ownership interest means ownership of/entitlement to more than 10% of the shares or capital or profits of the company.</p> <p>b) Control shall include the right or the ability 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.</p> <p>(ii) 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 10% of capital or profits of the partnership or who exercises control through other means.</p> <p>Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decisions.</p> <p>(iii) 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</p>

		<p>ownership of entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals.</p> <p>Explanation- Term 'Body of Individuals' includes Societies. Where no natural person is identified under (i), (ii) or (iii) above, the Beneficial Owner is the relevant natural person who holds the position of Senior Managing Official.</p> <p>(iv) Where the customer is a Trust, the identification of Beneficial Owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and other natural person exercising ultimate effective control over trust</p>
5	Certified Copy	<p>Obtaining a certified copy by the RE 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 RE as per the provisions contained in the Act and the rules thereunder.</p> <p>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:</p> <ul style="list-style-type: none"> • 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.
6	Cash Transactions	As defined under rule 3 of the Rules of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.
7	Central KYC Records Registry (CKYCR)	An entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. CKYCR is a reporting entity, substantially owned and controlled by the Central Government, and authorised by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client as referred to in clause (ha) in such manner and to perform such other functions as may be required under these rules.
8	Common Reporting Standards (CRS)	Common Reporting Standards (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
9	Customer	A Customer is a person, as defined below, who is engaged in a financial transaction or activity with a Housing Finance Company (HFC) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting. (Person is defined below in point no. 26)

10	Customer Due Diligence (CDD)	Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.
-----------	-------------------------------------	--

		<p>Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:</p> <p>(a) 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;</p> <p>(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;</p> <p>(c) 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.</p>
11	Customer Identification	Customer Identification means undertaking the process of CDD.
12	Designated Director	<p>A person designated by 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.</p> <p>For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.</p>
13	Digital KYC	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 the RE as per the provisions contained in the Act and in accordance with the rules and regulations specified in this behalf.
14	Digital Signature	Digital Signature shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
15	Domestic and cross-border wire transfer	When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.
16	Equivalent e-document	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.

17	FATCA	FATCA means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
18	Inter-Governmental Agreement (IGA)	"IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
19	Know Your Client (KYC) Identifier	The unique number or code assigned to a customer by the Central KYC Records Registry. (also called as KYC Identifier Number (KIN) or CKYCR No).
20	KYC Templates	KYC Templates means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for Individuals and Legal Entities.
21	Non-face-to-face	Customers who open accounts without visiting the branch/ offices of the RE or meeting the officials of RE.
22	Non-Profit Organisations (NPO)	NPO means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income- tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013

23	Officially Valid Document (OVD)	<p>Officially Valid Document (OVD) means:</p> <ol style="list-style-type: none"> a) Passport, b) Driving License, c) Voter’s Identity Card issued by Election Commission of India, d) Proof of possession of Aadhaar Number*, i.e. Aadhaar letter, Aadhaar Letter downloaded from UIDAI website (e-Aadhaar), Aadhaar Card, Aadhaar Secure QR Code, Aadhaar Paperless Offline e-KYC (an XML document generated by the UIDAI), (*Ensure to redact/ blacken only the first eight digits of Aadhaar No. (on copy of Aadhaar Letter/ Aadhaar Card obtained) e) Job Card issued by NREGA duly signed by an officer of the State Government, f) Letter issued by the National Population Register containing details of Name, Address of the customer with photograph of the card holder. <p>Provided that,</p> <ol style="list-style-type: none"> a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: - <ol style="list-style-type: none"> i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. property or Municipal tax receipt; iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector iv. Undertakings, if they contain the address; v. 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 d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. <p>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.</p>
----	--	---

24	Ongoing Due Diligence	Regular monitoring of transactions in accounts to ensure that those are consistent with the Company's knowledge about the customers, customers' business & risk profile, the source of funds / wealth.
25	Offline verification	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).
26	Person	Person has the same meaning assigned in the Act and includes: a) an Individual, b) a Hindu undivided family, c) a Company, d) a Firm, e) an Association of Persons or a Body of Individuals, whether incorporated or not, f) every artificial juridical person, not falling within any one of the above persons (a to e), and g) any Agency, Office or Branch owned or Controlled by any of the above persons (a to f).
27	Periodic Updation	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.
28	Politically Exposed Persons (PEPs)	Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/ Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.
29	Principal Officer	Principal Officer means an officer designated by the Company, responsible for furnishing information as per Rule 8 of the Rules.
30	Regulated Entities (REs)	Regulated Entities means a) All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks' b) All India Financial Institutions (AIFIs) c) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs). d) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
31	Shell Bank	Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

32	Suspicious Transaction	<p>“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-</p> <ul style="list-style-type: none"> (i) 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 (ii) appears to be made in circumstances of unusual or unjustified complexity, or (iii) appears to have no economic rationale or bonafide purpose, or (iv) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism. <p>Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.</p>
33	Transaction	<p>Transaction” means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes —</p> <ul style="list-style-type: none"> (i) opening of an account, (ii) deposits, 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, (iii) the use of a safety deposit box or any other form of safe deposit, (iv) entering into any fiduciary relationship, (v) payment made or received in whole or in part of any contractual or other legal obligation, (vi) establishing or creating a legal person or legal arrangement.
34	Video based Customer Identification Process (V-CIP)	<p>An alternate method of customer identification with facial recognition and CDD by an official of the RE by undertaking seamless, secure, live real- time, informed- 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 through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated as on par with face-to-face CIP for the purpose of this Policy.</p>
35	Walk-in Customer	<p>Walk-in Customer means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.</p>
36	Wire Transfer	<p>Wire transfer means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.</p>
37	Group	<p>The term “group” shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961.</p>

4. Key Elements of the KYC-AML Policy:

The policy shall include following four key elements:

- (i) Customer Acceptance Policy;
- (ii) Risk Management;
- (iii) Customer Identification Procedures (CIP); and
- (iv) Monitoring of Transactions

4.1 Money Laundering and Terrorist Financing Risk Assessment:

- a) Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Company from time to time.

- b) The risk assessment will be properly documented and will be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

- c) The outcome of the exercise will be put up to the Board or any committee of the Board to which power in this regard has been delegated and will be available to competent authorities and self-regulating bodies.

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

5. Designated Director:

- (i) Designated Director means the Managing Director or a Whole-Time Director duly authorised by the Board of Directors, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The Designated Director shall be nominated by the Board of the Company.

- (ii) The name, designation and address of the Designated Director, including changes from time to time, shall be communicated to the Director, FIU-IND, National Housing Bank and RBI.
- (iii) In no case, the Principal Officer shall be nominated as the Designated Director.

6. Principal Officer:

- (i) The Principal Officer shall be a Senior Officer of the Company at the management level and shall be responsible for ensuring compliance, monitoring transactions, and sharing reporting information as required under the law/regulations.
- (ii) The name of the Principal Officer so designated, his designation and address including changes from time to time, shall be communicated to the Director, FIU-IND, National Housing Bank and RBI.

7. Compliance with KYC-AML Policy:

The Company shall ensure compliance with the KYC-AML Policy through:

- (i) The below mentioned officials shall constitute as Senior Management and will be responsible for effective implementation of KYC policies and procedures:
 - Chief Executive Officer
 - National Operations Head
 - Chief Compliance Officer
- (ii) Allocating responsibilities through a Delegation of Powers Policy and Matrix for effective implementation of policies and procedures.
- (iii) Appointing an Internal Auditor for Independent evaluation of the compliance functions of SMHFC's policies and procedures and verification of compliance with KYC/ Anti- Money Laundering (AML) policies and procedures.
- (iv) Submission of quarterly audit notes and compliance to the Audit Committee.

The Company shall not outsource the decision-making functions for determining compliance with KYC norms.

CHAPTER – III: CUSTOMER ACCEPTANCE POLICY

8. Customer Acceptance Policy:

The following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing Loan facilities. The guidelines in respect of Customer Acceptance in the Company will broadly include the following:

- (i) No account will be opened in anonymous or fictitious/ benami name. Company shall insist for sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.
- (ii) No account will be opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an

- STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- (iii) No transaction or account-based relationship will be undertaken without following the CDD procedure.
 - (iv) The mandatory information will be sought for KYC purpose while opening an account and during the periodic updation, as specified.
 - (v) Optional/ additional information, where such information requirement has not been specified in this KYC-AML Policy, will be obtained with the explicit consent of the customer.
 - (vi) CDD Procedure will be followed for all the joint account holders, while opening a joint account.
 - (vii) SMHFC shall apply the CDD procedure at the UCIC level. If an existing KYC compliant customer desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
 - (viii) Circumstances in which, a customer is permitted to act on behalf of another person/ entity, will be clearly spelt out.
 - (ix) Suitable system will be put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in chapter IX of the RBI master directions (Requirements/obligations under International Agreements - Communications from International Agencies).
 - (x) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
 - (xi) Where an equivalent e-document is obtained from the customer, SMHFC shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000)
 - (xii) Where Goods and Services Tax (GST) details are available, the GST number must be verified
 - (xiii) from the search/verification facility of the issuing authority.
 - (xiv) SMHFC will also use RBI/ NHB caution advices in determining the customer acceptance framework.
 - (xv) In the event the customer is permitted to act on behalf of another person/entity, SMHFC shall verify that the customer has the necessary authority to do so by scrutinizing the authorizing document/s;

The Company shall ensure that adoption of Customer Acceptance Policy and its implementation shall not result in denial of services to the general public, especially to those, who are financially or socially disadvantaged.

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

CHAPTER – IV: RISK MANAGEMENT

9. **Risk Management:**

- (i) For effective implementation of KYC-AML Policy, the Company will ensure proper co-ordination, communication and understanding among all its departments.

The Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing policies and procedures and ensuring their effective implementation. The Company in consultation with the Board will devise procedure for creating Risk Profiles of the existing and new customers and apply AML measures keeping in view the risk involved in a transaction, account or business relationship.

For Risk Management, the Company will have a risk-based approach and shall categorise the customers as **Low, Medium** and **High-Risk** category based on the assessment and risk perception of the Company.

- (ii) Risk Categorization may be undertaken on various parameters including:
- a) Customer's Identity (the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in);
 - b) Social/ Financial Status;
 - c) Nature and volume of business of the customer;
 - d) Workplace of customer and of his clients;
 - e) Quantum and tenure of Loan facility applied for and proposed schedule for repayment of Loan.
 - f) Nature of employment;
 - g) Business activity of the customer;
 - h) Location of customer and his/ its clients;
 - i) Mode of Payments - cash, cheque / monetary instruments, wire transfers, forex transactions, etc.
 - j) Credit History;
 - k) Geographical risk covering customers as well as transactions;
 - l) Delivery channel used for delivery of products/services; and
 - m) Type of products/services offered.
- (iii) 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.

SMHFC may at its discretion identify additional factors that it may wish to utilize for customer acceptance based on risk profile determined by SMHFC. Provided further that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

- (iv) The Company has in place document viz. 'Policy on KYC Risk Categorisation' and the Risk Categorisation of customers will be carried out as per the said document.

CHAPTER – V: CUSTOMER IDENTIFICATION PROCEDURE (CIP)

10. Customer Identification Procedure (CIP):

- (i) The Company shall undertake Identification of customers in the following cases:
- a) Commencement of an account-based relationship with the customer: At the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship.
 - b) When there is doubt about the authenticity or adequacy of the customer identification data obtained.
 - c) For customers that are natural persons, sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph.
 - d) For customers which are legal persons or entities, the legal status of the legal person/entity shall be verified through proper and relevant documents. For any person purporting to act on behalf of the legal person/entity, it has to be verified whether he is so authorized and his identification has to be verified. Also, the ownership and control structure of the customer shall be understood so as to determine the natural person(s) who ultimately controls the legal person.

- e) Selling third party products as agents, selling their own products and any other product for more than Rupees fifty thousand.
 - f) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
 - g) When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
 - h) Introduction shall not to be sought while opening accounts.
- (ii) Currently, SMHFC conducts CDD for verifying the identity of the customers at the time of commencement of an account-based relationship only internally. In case, if it decides to hire third parties to conduct the CDD, they will be relied on, subject to the following conditions:
- a) Records or the information of the **customer due diligence** carried out by the third party is **obtained immediately from the third party** or from the Central KYC Records Registry.
 - b) Adequate steps will be taken to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
 - c) The **third party is regulated**, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under PMLA.
 - d) The third party is not based in a country or jurisdiction assessed as high risk.
 - e) The **ultimate responsibility for CDD**, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall **rest with the Company**.

CHAPTER -VI: CUSTOMER DUE DILIGENCE (CDD) PROCEDURE:

11. Customer Due Diligence (CDD) Procedure in case of Individuals:

- (i) While undertaking CDD, following information will be obtained 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) he is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act 2016 (18 of 2016): or
 - (ii) The customer 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
 - (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; or
 - (ac) the KYC Identifier with an explicit consent to download records from CKYCR; **and**
- (ii) PAN or equivalent e-document thereof or Form No. 60 as defined in Income-Tax Rules, 1962, **and**
- (iii) 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:

(iv) Provided that here the customer has submitted:

- Aadhaar number under clause (a), notified under first proviso to sub-section (1) of section 11A of the PML Act, SMHFC shall carry out 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 a customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, self- declaration to that effect must be obtained from the customer.
- The proof of possession of Aadhaar number under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.
- An equivalent e-document of any OVD, the 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 under Digital KYC Process rules and regulations (**Annexure-D**).
- Any OVD or proof of possession of Aadhaar number under Clause 11 (i)(a)(ii)(ab) above where offline verification cannot be carried out, the Company shall carry out verification through Digital KYC as specified by the rules and regulations reproduced under **Annexure-D**.
- KYC Identifier under Clause 11 (i)(a)(ii)(ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with Section 23.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Company may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Explanation 1: The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such **customer redacts or blacks out only the first eight digit of** Aadhaar Number (on copy of Aadhaar Letter/ Aadhaar Card obtained) 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

(v) **List of Officially Valid Documents:**

- a) Passport, the validity of which has not expired.
- b) Driving License, which has not expired
- c) Voter's Identity Card issued by Election Commission of India,
- d) Proof of possession of Aadhaar Number*, i.e. Aadhaar letter, Aadhaar Letter downloaded from UIDAI website (e-Aadhaar), Aadhaar Card, Aadhaar Secure QR Code, Aadhaar Paperless Offline e-KYC (an XML document generated by the UIDAI), *(Ensure to redact/ blacken only the First Eight Digits of Aadhaar No. (on copy of Aadhaar Letter/ Aadhaar Card obtained)
- e) Job Card issued by NREGA duly signed by an officer of the State Government,
- f) Letter issued by the National Population Register containing details of Name, Address of the customer having photograph of the card holder.

(vi) In case the OVD furnished by the customer does not contain updated address, the following documents or the equivalent e-documents thereof shall be Deemed to be OVDs (DOVD) for the limited purpose of Proof of Address: -

- a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill),
- b) Property or Municipal tax receipt,
- c) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public-Sector Undertakings, if they contain the address,
- d) Letter 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.

Provided that in case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided further that the **customer shall submit updated OVD with current address within a period of three months** of submitting the above documents.

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.

(vii) A customer already having an account-based relationship with the Company, shall submit his Permanent Account Number or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily ceased to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, Company shall give the customer an accessible notice and a reasonable opportunity to be heard.

Explanation: - For the purpose of this clause, "temporary ceasing of operations" in relation an account means the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this clause;

In case of asset accounts, such as **loan accounts**, for the purpose of ceasing the operation in the account, only **credits shall be allowed**.

(viii) If a customer having an existing account-based relationship with the Company gives in writing to the company that he/ she does not want to submit his/her PAN or Form No. 60, as the case may be, the customer's account with the company shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer. The Company shall duly inform the customer about this provision while opening the account.

(ix) List of the nature and type of documents/ information that may be relied upon for customer identification pertaining to Individuals, Sole Proprietary Firms, Legal Entities-Company, Partnership Firm, Trust, Unincorporated Association/Body of Individuals, Juridical Persons, BO is given in the **Annexure-A**.

(x) Video Customer Identification Process (V-CIP)

The Company may undertake live V-CIP, to be carried out by an official of the RE, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent. The guidelines for carrying out V-CIP is given at **Annexure-C**.

(xi) Accounts Opened using OTP based e-KYC, in non-face-to-face mode: The Company currently does not open accounts in non-face-to-face mode. However, in case in the future the Company does decide to open accounts in no-face-to-face-mode it shall not open accounts based on the KYC documents downloaded from CKYCR where the other Regulated entity has opened account through OTP based e-KYC procedure in non-face-to-face mode. All the required KYC documents will be obtained from the customer in case any account is to be opened based on documents downloaded from CKYCR.

12. CDD Measures for Identification of Beneficial Owner (BO):

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 PMLA Rules to verify his/her identity shall be undertaken keeping in view the following:

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

CHAPTER – VII: ONGOING DUE DILIGENCE

13. Ongoing Due Diligence:

Ongoing monitoring is an essential element of effective KYC procedures and is equally essential for the Company to have a clear knowledge and understanding about the normal working pattern and activity of the customer so that the Company can identify all such unusual transactions which would fall outside the normal transactions of the customer. To achieve this purpose, ongoing monitoring is necessary. The extent of such monitoring will depend upon the level of risk involved in each case. Any transaction or activity of the customer which gives rise to suspicion will be given special attention. Such monitoring is important to keep a check on any act or omission of the customer which may amount to money laundering or support any act relating to user of finance for criminal activities.

- (i) The Company will keep a continuous vigil if any of the following acts or events are noticed in relation to the customer's approach or behaviour while dealing with the Company:
 - a) Reluctance of the customer to provide confirmation regarding his identity.
 - b) Loan money is used for purposes other than the one mentioned in the Loan application form and the real purpose is not disclosed to the Company.
 - c) Customer forecloses the Loan within 180 days of availing the Loan facility wherein the Loan tenure is more than 12 months.

- d) A customer suddenly pays a substantial amount towards partial repayment of the Loan after paying a few EMIs.
 - e) A customer deposits with Company substantial cash amount after his EMI cheques have bounced and/or insists for cash payment in future to repay the remaining Loan amount.
- (ii) The company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

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 being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. The periodic review of the risk categorisation of Construction Finance (CF) Loans shall also be at least once in six months or at an earlier frequency as determined by the relevant authority.

- (iii) For the purpose of risk categorization, the Company has put in place a separate document named "Policy for KYC Risk Categorisation". The indicative factors involved in Risk Categorisation may include, amongst other factors, the following:
- Individuals (other than High Net Worth) 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, may be categorized as low risk. Illustrative examples of low-risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments & Government owned companies, regulators and statutory bodies, etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met.
 - Customers that are likely to pose a higher-than-average risk to the SMHFC may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.
 - SMHFC may 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 which are used for business operations or sources to repay the Loan to the Company are not clearly disclosed or cannot be ascertained from the financial statements submitted by the customer to the Company.

Examples of customers requiring higher due diligence may include:

- Non-resident customers,
- High net worth individuals,
- Trusts, charities, NGOs and organizations receiving donations,
- Companies having close family shareholding or beneficial ownership,
- Firms with 'sleeping partners',
- Politically exposed persons (PEPs),
- Non-face to face customers, and
- Persons with dubious reputation as per the public information available.

14. Periodic Updation:

A. Periodic KYC updation shall be carried out **at least Once** in:

- Every **two years** for **High-Risk** customers,
- Every **eight years** for **Medium-Risk** customers and
- Every **ten years** for **Low-Risk** customers.

The time limits prescribed above would apply from the date of opening of the account / last verification of KYC.

Policy in this regard is as below:

a) Periodic Updation of Individual Customers:

i. No change in KYC information:

In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with SMHFC, customer's mobile number registered with the Company, digital channels (such as online banking/ internet banking, mobile application of SMHFC), letter, etc.

ii. Change in address:

In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the SMHFC, customer's mobile number registered with the SMHFC, digital channels (such as mobile application of SMHFC), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, the Company at its option may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

b) Customers other than Individuals:

i. No change in KYC information:

In case of no change in the KYC information of the Legal Entities (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, digital channels (such as online banking/ internet banking, mobile application of SMHFC), letter from an official authorized by the LE in this regard, board resolution etc. Further, SMHFC shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to date as possible.

ii. Change in KYC information:

In case of change in KYC information, SMHFC shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

c) Additional measures: In addition to the above, SMHFC shall ensure that,

- i. The KYC documents of the customer as per the current CDD standards are available with it. This is applicable even if there is no change in customer information but the documents available with SMHFC are not as per the current CDD standards. Further, in case the validity of the CDD documents available with SMHFC has expired at the time of periodic updation of KYC, SMHFC shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

- ii. The customer's PAN details, if available with the Company shall be verified from the database of the issuing authority at the time of periodic updation of KYC.
- iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records/ database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- iv. In order to ensure customer convenience, SMHFC may consider making available the facility of periodic updation of KYC at any office, in terms of the KYC-AML Policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated.
- v. The company shall adopt a risk-based approach with respect to 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. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the KYC-AML Policy duly approved by the Board of Directors of SMHFCs or any committee of the Board to which power has been delegated.
- vi. The company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at company's end.

- B. In case of existing customers, SMHFC shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which SMHFC shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, SMHFC shall give the customer accessible notice and a reasonable opportunity to be heard.

Further, Management Committee of SMHFC will provide appropriate relaxation for continued operation of accounts of customers who are unable to provide Permanent Account Number or Form No.60 owing to injury, illness, or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with SMHFC gives in writing to that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, SMHFC shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, “temporary ceasing of operations” in relation to an account shall mean the temporary suspension of all transactions or activities in relation to that account by SMHFC till such time the customer complies with the provisions of this Section. In the case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

15. Enhanced Due Diligence Measures:

- (i) **Accounts of non-face-to-face customers:** Currently, the Company does not open accounts through non-face-to-face mode. However, in future in case the Company decides to open accounts using such mode, it shall follow the below-mentioned process for enhanced due diligence of such accounts.

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

- a) In case company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. RE shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
- c) Apart from obtaining the current address proof, company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

The guidelines for carrying out V-CIP is given at **Annexure-C**.

- (ii) **Accounts of Politically Exposed Persons (PEPs):** The Company shall have the option of **establishing** a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

- a) Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP
- b) Reasonable measures are taken to obtain sufficient information including information about the sources of funds / wealth accounts of family members and close relatives is gathered on the PEP,
- c) the decision to open an account for a PEP is taken at a Senior management level in accordance with the Company’s Customer Acceptance Policy,

- d) all such accounts are subjected to enhanced monitoring on an on-going basis,
- e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, Senior Management's approval is obtained to continue the business relationship,

These instructions shall also be applicable to family members or close associates of PEPs

The above instructions will also be applicable to accounts where a PEP is the Beneficial Owner.

(iii) Customer's Accounts Opened by Professional Intermediaries:

Currently, the Company does not employ any intermediaries to open accounts with the Company. However, in case the Company decides to employ such intermediaries, it shall follow the below-mentioned enhanced Due Diligence process.

- i. SMHFC shall ensure the identification of all beneficial owners in respect of such accounts.
- ii. Further SMHFC shall also ensure that the CDD conducted by the intermediaries is in line with KYC requirements mandated by RBI.
- iii. SMHFC shall ensure that no professional intermediary who cannot reveal the identity of a customer should be allowed to open such an account with it.
- iv. Company will have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- v. SMHFC shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the SMHFC.
- vi. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of SMHFC, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of SMHFC, the SMHFC shall look for the beneficial owners.
- vii. The Company shall, at its 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.
- viii. The ultimate responsibility for knowing the customer lies with the Company.

CHAPTER - VIII: RECORD MANAGEMENT

16. Maintenance of Records of Transactions (nature and value):

- (i) The company shall maintain proper record of the transactions (nature and value), in such form and for such period as specified under the Rule 3 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. The Company shall maintain record of all transactions including the record of:
 - a) All cash transactions of the value of more than Rupees Ten lakh or its equivalent in foreign currency.
 - b) All series of cash transactions integrally connected to each other which have been individually valued below Rupees Ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate value of such transactions exceeds Rupees Ten lakh.
 - c) All transactions involving receipts by Non-Profit Organizations of value more than ₹ 10 lakhs, or its equivalent in foreign currency.

- d) 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.
 - e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- (ii) The company will maintain and preserve all necessary information in respect of transactions as prescribed above under Rule 3 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, so as to permit reconstruction of individual transaction which shall also include 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 and
 - d) The parties to the transaction.
- (iii) The Company will take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows information to be retrieved easily and quickly whenever required or requested by the competent authorities.
- (iv) As per the provisions of PMLA, the Company shall maintain records as under:
- a. Records of the identity and address of all clients and beneficial owners, obtained while onboarding and updated thereafter, for a period of five years from the date of cessation of relationship.
 - b. Records of all transactions for a period of five years from the date of transaction.
- (v) In case of customers who are non-profit organisations, the details of such customers shall be registered on the DARPAN Portal of NITI Aayog. Such registration records shall be maintained for a period of five years after the business relationship between the customer and SMHFC has ended or the account has been closed, whichever is later.

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.

CHAPTER VIII: REPORTING REQUIREMENTS

17. **Reporting to Financial Intelligence Unit-India (FIU-IND):**

- (i) In terms of the provisions of the Rule 7 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. Company shall, inter-alia, furnish to the Director FIU-IND as mentioned in above point (Rule 3 of PML (Maintenance of Records) Rules, 2005).
- (ii) A copy of information furnished shall be retained by the 'Principal Officer' for the purposes of official record.
- (iii) 'NIL' report need not be submitted in case there are no Cash / Suspicious Transactions.
- (iv) Company shall prepare the reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility

developed by FIU. Company shall use the editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) for extracting CTR /STR from their live transaction data.

- (v) No restrictions will be put on account operations where an STR has been filed.
- (vi) Robust software/system developments, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers will be put in to use as a part of effective identification and reporting of suspicious transactions.
- (vii) While furnishing of information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.
- (viii) The Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of the KYC Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

An illustrative list of suspicious transactions in housing / builder / project loans is given at **Annexure-E**.

CHAPTER X: REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGENCIES

18. Section 51A of Unlawful Activities (Prevention) (UAPA) Act, 1967

- a) SMHFC shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:
 - (i) The “**ISIL (Da’esh) & Al-Qaida Sanctions List**”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.
 - (ii) The “**1988 Sanctions List**”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the **Taliban** which is available at <https://www.un.org/securitycouncil/sanctions/1988/materials>
- b) The details of accounts resembling any of the individuals/entities in the above mentioned lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated Feb 2,2021.
- c) The Company shall also verify every day, the ‘**UNSCR 1718 Sanctions List** of Designated Individuals and Entities’, as available at <https://www.un.org/securitycouncil/sanctions/1718/materials> & UNSC sanctions lists on Iran as available at <https://www.un.org/securitycouncil/content/2231/list>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the ‘Implementation of Security Council Resolution on Democratic People’s Republic of Korea Order, 2017’, as amended from time to time by the Central Government.
- d) In addition to the above, SMHFC shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.
- e) Company shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

19. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated February 2, 2021 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

20. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

- i. Company shall ensure meticulous compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 01, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).
- ii. The company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
- iii. 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.
- iv. Company shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- v. In case of match in the above cases, company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to the State Nodal Officer, where the account / transaction is held and to the RBI. The Company shall file an STR with FIUIND covering all transactions in the accounts covered above, carried through or attempted.
- vi. In case of doubt, the company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
- vii. In case an order to freeze assets under Section 12A is received by the company from the CNO, Company shall, without delay, take necessary action to comply with the Order.
- viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

21. Jurisdictions that do not or insufficiently apply the FATF Recommendations

- a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Company shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
- b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 55 a & b do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement

- c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.
- d) Financial Action Task Force (FATF) Listed Countries/ Jurisdictions: (<http://www.fatf-gafi.org/>) (subject to change).

CHAPTER – XI: OTHER MEASURES

22. Secrecy Obligations and Sharing of Information:

- (i) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.
- (ii) The exceptions to the said rule shall be as under:
 - Where disclosure is under compulsion of law;
 - Where there is a duty to the public to disclose;
 - The interest of the Company requires disclosure; and
 - Where the disclosure is made with the express or implied consent of the customer.
- (iii) While considering the requests for data/information from Government and other agencies, Company will satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in transactions.
- (iv) The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

23. Customer Due Diligence Procedure and Sharing KYC information with Central KYC Records Registry (CKYCR):

- i. The Company will capture the KYC information, for sharing with the CKYCR as mentioned in the Rules, as per their KYC templates for 'individuals' and 'Legal Entities'. The Company will upload the KYC data with CKYCR in respect of new individual accounts opened on or after April 1, 2017.
- ii. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- iii. In terms of provision of Rule 9 (1A) of PML Rules, SMHFC shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- iv. The Company shall upload KYC records pertaining to accounts of Legal Entities ("LEs") opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records shall be uploaded as per the LE Template released by CERSAI.
- v. Once the KYC Identifier is generated by CKYCR, SMHFC shall ensure that the same is communicated to the Individual/ Legal Entity as the case may be.
- vi. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, SMHFC shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per (i) and (iv) respectively at the time of periodic updation as specified in Section 15 of this policy, or earlier, when the updated KYC information is obtained/received from the customer.
- vii. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

- viii. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to SMHFC, with an explicit consent to download records from CKYCR, then SMHFC 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) the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client;
 - (d) The validity period of documents downloaded from CKYCR has lapsed.
- ix. On update of a customer record being processed at the Central KYC Registry, all linked financial institutions (institutions that have either uploaded or downloaded the KYC record for that customer), will receive an electronic update notification of KYC record from CKYCR. The Company shall download from CKYCR such last updated record of the customer.

24. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS):

- (i) Under FATCA and CRS, SMHFC shall adhere to the provisions of Income Tax Rules 114F, 114G, 114H, if applicable. Currently SMHFC is not a Reporting Financial Institution (RFI) as defined in Income Tax Rule 114F. However, in case SMHFC comes within the purview of the said Rule it shall take following steps for complying with the reporting requirements:
 - (a) Register on the related e-filing portal of Income Tax Dept. as RFI at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution.
 - (b) Submit online reports using digital signature of the 'Designated Director' by uploading the Form 61B or 'NIL' report, for which, the scheme of Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation – Company will refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://wwwfedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules.
 - (c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
 - (d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
 - (e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance. The committee shall comprise of Chief Financial Officer (Chairperson), Finance Controller & Chief Compliance Officer as members and shall meet atleast annually with a quorum of atleast 2 out of 3 members.
 - (f) Company shall ensure compliance with updated instructions/ rules/ guidance notes/Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

25. Unique Customer Identification Code:

The Company shall allot an Unique Customer Identification Code (UCIC) while entering into new relationships with Individual customers as also the existing customers of the Company. (Company shall, at its option, not issue UCIC to all walk-in/occasional customers such as purchasers of third-party products provided it is ensured that there is adequate mechanism to identify such walk- in customers who have frequent transactions with them and ensure that they are allotted UCIC).

26. Introduction of New Technologies –

Company shall identify any money-laundering and financing of terrorism threats that may arise in relation to the development of new products and new business practices including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Accordingly, company shall undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services and technologies; and take appropriate measures to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

27. 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, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

28. Selling Third party products:

Currently the company is not engaged in selling third-party products. However, in case it decides to engage in selling third party products as agents, the Company shall comply with the applicable laws/regulations, including system capabilities for capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers.

- a) Identity and address of the walk-in customer shall be verified for transactions above Rupees fifty thousand.
- b) Transaction details of sale of third-party products and related records shall be maintained as prescribed in Section 46 of Chapter VII of the RBI KYC Master Directions.
- c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
- d) Transactions involving rupees fifty thousand and above shall be undertaken only by:
 - Debit to customers' account or against cheques; and
 - Obtaining and verifying the PAN given by the account-based as well as walk-in customers.
- e) Instruction at 'd' above shall also apply to sale of SMHFC's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

29. Hiring of Employees and Employee training:

- (i) Adequate screening mechanism as an integral part of personnel recruitment/ hiring process to be in place.
- (ii) On-going employee training programme be in place so that the members of staff are adequately trained in KYC & AML Measures policy. The focus of the training be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff will be specially trained to handle issues arising from lack of customer education.
- (iii) SMHFC shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up

with the changing KYC/AML/CFT landscape, nationally and internationally. SMHFC must also seek to create an environment that encourages open communication and high integrity among its employees.

- (iv) Proper staffing of the audit function with persons adequately trained and well-versed in KYC / AML / CFT policies of the company, regulations and related issues should be ensured.

30. Review of Policy:

The Board shall have the right to amend the Know Your Customer and Anti-Money Laundering Policy from time to time. The Policy shall be reviewed annually along with the other policies. However, changes, if any, will be made in the Policy from time to time based on the changes in Regulatory and Statutory Guidelines, various laws including Prevention of Money Laundering Act, 2002 and RBI guidelines.

* * *

ANNEXURES

ANNEXURE-A

Customer Identification Procedure

KYC Documents to be obtained for Opening various type of Accounts which are based on the RBI guidelines, PMLA/PML Rules and UIDAI Notifications are given below:

(A) KYC Documents for an Account of INDIVIDUAL, (including BENEFICIAL OWNER, AUTHORIZED SIGNATORY and POWER OF ATTORNEY HOLDER;))

- (1) One recent **Photograph**,
- (2) **PAN** or Form 60 if PAN is not allotted
- (3) **Certified Copy** * of one of the Officially Valid Documents (**OVDs**) listed below:

Sr.	Officially Valid Documents
1	Passport
2	Driving License
3	Voter's Identity Card issued by Election Commission of India
4	Proof of possession of Aadhaar Number i.e. Aadhaar Letter, Aadhaar Letter downloaded from UIDAI website (e-Aadhaar), Aadhaar Card, Aadhaar Secure QR Code, Aadhaar Paperless Offline e-KYC (an XML document generated by the UIDAI) **
5	Job Card issued by NREGA duly signed by an officer of the State Government
6	Letter issued by the National Population Register containing details of Name, Address of the customer with photograph of the card holder.
* Obtaining a Certified Copy by Reporting Entity (includes SMHFC) means comparing the copy of Officially Valid Document (OVD) so produced by the client (i.e. customer) with its Original and recording the same on the copy by the authorised officer of the Reporting Entity” Copies of the KYC Documents should be Self- attested by the customers.	
** Ensure to redact/ blacken only the first eight digits of Aadhaar No. (on copy of Aadhaar Letter/ Aadhaar Card obtained).	

- (4) In case **OVD** does not have **Current Address** of the client, obtain below listed documents which are treated

Deemed to be Officially Valid Documents (DOVD) for the limited purpose of Proof of Address:

Sr. No.	Deemed to be Officially Valid Documents (DOVD) - Proof of Address (PoA)
i	Utility bill , in the name of the client, which is not more than two months old of any service provider (Electricity, Telephone, Post-paid Mobile Phone, Piped Gas, Water bill)
ii	Property or Municipal tax receipt
iii	Pension or Family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public-Sector Undertakings, if they contain the address
iv	Letter of Allotment of Accommodation from Employer issued by State Government or Central Government Departments, Statutory or Regulatory Bodies, Public Sector Undertakings, Scheduled Commercial Banks, Financial Institutions and Listed Companies, and Leave & License Agreements with such employers allotting official accommodation

In case a client submits Deemed to be OVD (DOVD) towards Current Address, client must submit an OVD mentioned in **(A)(3)**, updated with Current Address, within **three months** of submission of the DOVD.

(B) KYC Documents for an Account of SOLE PROPRIETARY FIRMS:

- 1) **KYC Documents** of the **Proprietor** as per the KYC Documents for Individual mentioned in **Point A** and
- 2) **Any** of the **Two** documents in the name of the Proprietorship Concern as **Proof of Business Activity** mentioned below:

Sr. No.	Proof of Business/ Activity in the name of the Proprietorship Concern
i	Registration Certificate including Udyam Registration Certificate issued by the government (Indicative list of Licenses / Certificates is given in Annexure - B)
ii	Certificate / License issued by the Municipal Authorities under Shop & Establishment Act
iii	Sales and Income Tax returns
iv	GST/ CST/ VAT certificate (Provisional / Final)
v	Certificate / Registration document issued by Sales Tax / Service Tax / Professional Tax Authorities
vi	The complete Income Tax return (not just the acknowledgement) in the Name of the Sole Proprietor where the firm's income is reflected and the same is duly authenticated/ acknowledged by the Income Tax Authorities
vii	Utility Bills such as Electricity, Water, and Landline Telephone bills in the Name of the Proprietary Concern

(C) KYC Documents or equivalent e-documents for an Account of PARTNERSHIP FIRM:

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr. No.	Document Name
i	PAN of the Firm
ii	Partnership Deed
lii	GST/ CST/ VAT certificate (Provisional / Final)
iv	Names of all the partners and any one KYC Documents for Individual mentioned in Point A of each partner
v	The registered office and the principal place of its business, if it is different, to be obtained on the Letterhead of the Firm signed by an Authorised Signatory.

(D) KYC Documents or equivalent e-documents for an Account of a COMPANY:

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr. No.	Document Name
i	PAN of the Company
ii	Certificate of Incorporation
iii	Memorandum and Articles of Association (MOA & AOA)
iv	GST/ CST/ VAT certificate (Provisional / Final)
v	Names of all the Directors and any one KYC Documents for Individual mentioned in Point A of each Director
vii	Names of the relevant persons holding senior management position
viii	The registered office and the principal place of its business, if it is different, to be obtained on the Letterhead of the Company signed by an Authorised Signatory.

(E) KYC Documents or equivalent e-documents for an Account of a LIMITED LIABILITY PARTNERSHIP

FIRM:

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr. No.	Document Name
i	PAN of the LLP
ii	Certificate of Incorporation
iii	Limited Liability Partnership Agreement
iv	List of all existing designated partners of the LLP along with the Designated Partner Identification Number (DPIN) issued by the Central Government (on the letterhead of the LLP)
v	Any one KYC Documents for Individual mentioned in Point A of all the Designated Partners
Vi	The registered office and the principal place of its business, if it is different, to be obtained on the Letterhead of the Firm signed by an Authorised Signatory.

(F) KYC Documents or equivalent e-documents for an Account of TRUST:

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr. No.	Document Name
i	PAN or Form 60 of the Trust
ii	Trust Deed
iii	GST/ CST/ VAT certificate (Provisional / Final)
iv	Names of all the trustees and any one KYC Documents for Individual mentioned in Point A of each Trustee

(G) KYC Documents or equivalent e-documents for an Account of an UNINCORPORATED ASSOCIATION OR BODY OF INDIVIDUALS (includes **SOCIETIES):**

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr.	Document Name
i	PAN or Form 60 of the unincorporated association or a body of individuals
ii	GST/ CST/ VAT certificate (Provisional / Final)
iii	Such information as may be required to collectively establish the legal existence of such Association or Body of Individuals

(H) KYC Documents or equivalent e-documents for an Account of HINDU UNDIVIDED FAMILY (HUF):

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

Sr.	Document Name
i	PAN of HUF
ii	GST/ CST/ VAT certificate (Provisional / Final)
iii	Names of the karta and all the co-parceners and any one KYC Documents for Individual mentioned in Point A of the Karta and each co-parcener.

(J) Clarification / Instructions:

Sr. No.	Particulars
i	Beneficial Owner (BO) is a Natural Person(s) (i.e. individual) 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. In case of account of a legal entity, BO must be identified and verified at the time of on boarding of a customer by obtaining KYC Documents as listed in Point (A). Provided that in case of a trust, the trustees are required to disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clause (b) of sub-rule (1) rule 9 under the PML Rules when transactions are carried out through a juridical person.
ii	While obtaining copy of Aadhaar letter, Aadhaar card, etc. the Aadhaar Number must be redacted or blackened so that it is not legible .
iii	In case, where a client has submitted Deemed to be OVD (DOVD) towards Current Address, such client must submit an OVD updated with Current Address within three months of submission of the DOVD documents.
iv	OVDs and Deemed to be OVDs should be in the name of the client (i.e. customer)
v	Attorney holder means Trustee, Manager, Officer, Employee, Authorised Signatory, etc. holding an Attorney to transact on behalf of the client as per Point (A).
vi	Photograph, Photocopy of the OVD/DOVD or any documents obtained must be clear & legible.
vii	PAN is a mandatory document in case of Account of Company and Partnership Firm. Form 60 in lieu of PAN can be considered for entities/individuals other than company & partnership firm.
viii	PAN verification from the verification facility available with the issuing authority
ix	Aadhaar is an Officially Valid Document (OVD) as per the Prevention of Money-Laundering (Maintenance of Records) Amendment Rules, 2019 dated February 13, 2019.

Annexure - B

<u>Indicative List of Licenses / Certificates Issued in the Name of the Proprietary Firm by any Professional Body Incorporated under a Statute</u>	
Sr. No.	Type of Document
i	Full Fledge Money Changer (FFMC) Licence issued by RBI.
ii	Small Scale Industries Certificate: Trade Licence issued by Department of Industries and Commerce.
iii	Permission issued by respective Government Authority for units in SEZ (Special Economic Zone), STP (Software Technology Park), EOU (Export Oriented Unit), EHTP (Electronic Hardware Technology Park), DTA (Domestic Tariff Area) and EPZ (Export Processing Zone).
iv	Registration Certificate of recognised Provident Fund with PF Commissioner.
v	Permission to carry out business issued by Village Administrative Officer / Panchayat Head / Mukhiya / Sarpanch / Talati / Village Developmental Officer / Block Development Officer or Equal Rank officer for customers in rural / village areas and President / CEO if the document is issued by Nagar Parishad / Zilla Parishad. Branch to ascertain and ensure that the official who has signed the certificate has been
vi	Factory Registration Certificate issued by any State / Central Government Authority.

vii	Licence to sell stock or exhibit for sale or distribute insecticides, under the Insecticides Rules, issued by respective State / Union Government Department.
viii	Licence issued under Contract Labour (Regular & Abolition) Act 1970. If generated online it should be attested by Municipal Authorities.
ix	Licence issued by Police Department under the provisions of State Police Acts.
x	Zilla Udyog Kendra Registration Certificate.
xi	Registration for Fire Goods issued by Municipal Corporations.
xii	Trade Licence from Labour Department.
xiii	Certificate issued by ANCHAL SAMITI MEMBER for existence of Firm. The Anchal Samiti exists at the Block level in Arunachal Pradesh and is a body under the Panchayati Raj system for a cluster of villages.
xiv	APMC / Mandi License / Certificate and as part of due diligence, please obtain the receipt for amount paid to the concerned authority for issuance/ renewal of this license.
xv	Gram Panchayat Certificate (should be on letterhead and not more than 3 months old).

Annexure - C

Video Based Customer Identification Process (V-CIP)

A. The Company may undertake V-CIP to carry out:

- i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, SMHFC shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Annexure A apart from undertaking CDD of the proprietor.
- ii. Updation /Periodic updation of KYC for eligible customers.
- iii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e- KYC authentication.

The Company while undertaking V-CIP, shall adhere to the following minimum standards:

a) **V-CIP Procedure**

- i. The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure shall be housed in the own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology-related outsourcing for the process should be compliant with relevant RBI guidelines.
- ii. The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer's consent should be recorded in an auditable and alteration proof manner.
- iii. The V-CIP infrastructure/ application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iv. The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
- v. The application shall have components with face liveness / spoof detection as well as face matching technology with a high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- vi. Based on experience of detected/ attempted/ 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be

regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

- viii. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance with internal / regulatory guidelines.
- ix. The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in a live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

b) V-CIP Procedure

- (i) The Company shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
- (ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption does not lead to the creation of multiple files, then there is no need to initiate a fresh session by the company. However, in case of call drop / disconnection, fresh session shall be initiated.
- (iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
- (iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.
- (v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.
- (vi) The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
 - a) Offline Verification of Aadhaar for identification
 - b) KYC records downloaded from CKYCR, in accordance with Section 24, using the KYC identifier provided by the customer
 - c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi locker.

The Company shall ensure to redact or blackout the first eights of Aadhaar number.

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 working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, SMHFC shall ensure that the video process of the V-CIP is undertaken within three working days of downloading/ obtaining the identification information through CKYCR / Aadhaar authentication/ equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, SMHFC shall ensure that no incremental risk is added due to this.

- (vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that

the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

- (viii) The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi locker.
- (ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
- (x) The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
- (xi) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.
- (xii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

c) V-CIP Records and Data Management

- i. The entire data and recordings of V-CIP shall be stored in a system / system's located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in the RBI Master Direction on KYC, shall also be applicable for V-CIP.
- ii. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

Annexure - D

Digital KYC Process

- A. The RE shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the REs.
- B. The access of the Application shall be controlled by the REs and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by REs to its authorized officials.
- C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
- D. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- E. The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- 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 registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
- 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 the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
- 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 RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.
- L. The authorized officer of the RE 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 of the RE 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.

Annexure - E

Illustrative List of Suspicious Transactions

A. Builder/ Project/ Corporate Clients

1. Builder approaching the HFC for a small loan compared to the total cost of the project.
2. Builder is unable to explain the sources of funding for the project.
3. Approvals/sanctions from various authorities are proved to be fake or if it appears that client does not wish to obtain necessary governmental approvals/ filings, etc.
4. Management appears to be acting according to instructions of unknown or inappropriate person(s).
5. Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
6. Clients with multi-jurisdictional operations that do not have adequate centralised corporate oversight.
7. Advice on setting up of legal arrangements that may be used to obscure ownership or real economic purpose (including setting up of Trusts, Co., change of name/corporate seat or other complex group structures).
8. Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.

B. Individuals

1. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
2. Unnecessarily complex client structure.
3. Individual or classes of transactions that take place outside the established business profile and expected activities/ transaction unclear.
4. Customer is reluctant to provide information, data, documents.

5. Submission of false documents, data, purpose of loan, details of accounts.
6. Refuses to furnish details of source of funds for initial contribution, sources of funds is doubtful etc.
7. Reluctant to meet in person, represents through a third party/POA holder without sufficient reasons.
8. 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.
9. Unable to explain or satisfy the numerous transfers in the statement of account/ multiple accounts.
10. Initial contribution made through unrelated third-party accounts without proper justification.
11. Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount.
12. Suggesting dubious means for the sanction of loan.
13. Where transactions do not make economic sense.
14. Unusual financial transactions with unknown source.
15. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
16. There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased.
17. Encashment of loan amount by opening a fictitious bank account.
18. 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.
19. Sale consideration in the sale agreement is abnormally higher/lower than prevailing in the area of purchase.
20. Multiple funding of the same property/dwelling unit.
21. Request for payment made in favour of a third party who has no relation to the transaction.
22. 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.
23. Multiple funding -financing involving NCO/Charitable Organisation /SMEs/SHGs/Micro Finance Groups.
24. Frequent requests for change of address.
25. Overpayment of instalments with a request to refund the overpaid amount.
26. Investment in real estate at a higher/lower price than expected.
27. Clients incorporated in countries that permit bearer shares