Svatantra Micro Housing Finance Corporation Limited

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

- May 1st, 2026

	Authorized Person
Title	Know Your Customer (KYC) – Anti-Money Laundering (AML) Policy (Ver. 5.0)
Drafted by	Tasneem Rangwala (Company Secretary)
Reviewed by	Kashyap Patel (National Credit and Operations Head)
Approved by	Deepabh Jain (Chief Executive Officer)

Know Your Customer and Anti-Money Laundering Policy

Version Control	Effective Date	Changes Effected
1.0	April 1, 2020	Annual review
1.1	April 1, 2021	Annual review
1.2	April 1, 2022	Annual review
1.3	April 1, 2023	Annual review
2.0	April 1, 2024	Revised pursuant to amendment RBI Master Direction – Know Your Customer (KYC) Direction, 2016 updated on January 04, 2024.
3.0	February 14, 2025	To amend Annexure-A for addition of documents in case of Partnership Firm, Company and Trust.
4.0	January 21, 2026	Revised pursuant to amendment circulated by Reserve Bank of India (RBI) vide - - Circular No. RBI/DOR/2025-26/361 DOR.AML.REC.No.280/14.01.003/2025-26 Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated 28th November 2025 and - Circular DOR.AML.REC.364/14.01.003/2025-26 Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Amendment Directions, 2025 dated 29th December 2025.
5.0	May 01, 2026	Change in Income Tax Rules references in the Policy due to introduction of Income Tax Rules 2026.

CHAPTER - I: INTRODUCTION

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.

This policy has been revised pursuant to latest amendment circulated by Reserve Bank of India (RBI) vide circular No. RBI/DOR/2025-26/361 DOR.AML.REC.No.280/14.01.003/2025-26 Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated 28th November, 2025 (hereinafter called "Directions") and amendment vide circular DOR.AML.REC.364/14.01.003/2025-26 Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Amendment Directions, 2025 dated 29th December 2025.

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	shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
2.	Act and Rules	mean the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
3.	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)**	(a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has / have a controlling ownership interest or who exercises control through other means. Explanation: For the purpose of this sub-clause- ● 'Controlling ownership interest' means ownership of / entitlement to more than 10 percent of the shares or capital or profits of the company. ● 'Control' shall include the right to appoint the majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements. (b) 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(s), has / have ownership of / entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means. Explanation: For the purpose of this sub-clause, 'control' shall include the right to control the management or policy decision. (c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has / have ownership of / entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals. Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official. (d) 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 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

5.	**Certified Copy**	The Company obtaining the certified copy shall mean comparing the copy of the proof of possession of Aadhaar number (where offline verification cannot be carried out) or the officially valid document produced by the customer with the original, and an authorised officer of the Company shall record the comparison on the copy as per the provisions contained in the Act. 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)}, the Company may alternatively obtain the original certified copy, certified by any one of the following: a. authorised officials of overseas branches of Scheduled Commercial Banks registered in India, b. branches of overseas banks with whom Indian banks have relationships, c. Notary Public abroad, d. Court Magistrate, e. Judge, f. 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)**	means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
8.	**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**	means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

10.	**Customer Due Diligence (CDD)**	means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. 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 ₹50,000 whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include: (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 (b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control; (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.
11.	**Customer Identification**	means undertaking the process of CDD.
12.	**Designated Director**	means a person whom the Company designates 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, whom the Board of Directors has duly authorised. Explanation: 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.
13.	**Digital KYC**	shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
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**	**Domestic wire transfer** refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfers that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country. **Cross-border wire transfer** refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

16.	**Equivalent e-document**	means an electronic equivalent of a document that the issuing authority of such document issues 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**	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)**	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.	**Group**	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 (43 of 1961).
20.	**Know Your Client (KYC) Identifier**	means the unique number or code that the Central KYC Records Registry assigns to a customer. Explanation: A customer can obtain his KYC Identifier through the following ways: In the process of opening an account, once the customer's KYC Identifier is generated by CKYCR and provided to the Company, the latter shall share the same with the concerned customer. The customer can also access his KYC Identifier on CKYCR Portal (www.ckycindia.in).
21.	**KYC Templates**	means templates prepared to facilitate collating and reporting KYC data to the CKYCR, for individuals and legal entities.
22.	**Non-face-to-face Customers**	means customers who open accounts without visiting the branch / offices of the Company or meeting the officials of the Company.
23.	**Non-Profit Organisations (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 (18 of 2013).
24.	**Officially Valid Document (OVD)**	Means: 1. the passport, 2. the driving licence, 3. proof of possession of Aadhaar number, 4. the Voter's Identity Card that the Election Commission of India issues, 5. the job card that NREGA issues and an officer of the State Government duly signs, and 6. the letter that the National Population Register issues containing details of name and address. Provided that,

		a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form that the Unique Identification Authority of India (UIDAI) issues. b) When the customer furnishes an OVD that does not have an updated address, the Company shall deem the following documents or the equivalent e-documents thereof to be OVDs for the limited purpose of proof of address :- ● utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ● property or Municipal tax receipt; ● pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; ● letter of allotment of accommodation from employer that is 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; Illustration: If a customer is staying in Chennai but their OVD contains an address in New Delhi, they can open an account in Chennai by submitting a deemed to be OVD for the purpose of proof of address. However, as mentioned below in clause (c), they are required to submit an OVD with current address within a period of three months. (c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at (b) above (d) if the OVD that a foreign national presents does not contain the details of address, the Company shall accept documents that Government departments of foreign jurisdictions issue, and a letter that the Foreign Embassy or Mission in India issues, as proof of address. Explanation: For the purpose of this clause, the Company shall deem a document to be an OVD even if there is a change in the name subsequent to its issuance provided that it is supported by a marriage certificate that the State Government issues or a Gazette notification, indicating such a change of name.
25.	**Ongoing Due Diligence**	means regular monitoring of transactions in accounts to ensure that transactions are consistent with the Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
26.	**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).

27.	**Person**	has the same meaning assigned in the Act and includes: (a) an individual, (b) a Hindu undivided family, (c) a company, (d) an association of persons or a body of individuals, whether incorporated or not, (e) every artificial juridical person, not falling within any one of the above persons (a to e), and (f) any agency, office or branch owned or controlled by any of the above persons (a to f).
28.	**Periodic Updation**	means the steps taken to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the RBI.
29.	**Politically Exposed Persons (PEPs)**	are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States / Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.
30.	**Principal Officer**	means the Company's nominated officer at the management level, responsible for furnishing information as per rule 8 of the Rules.
31.	**Regulated Entities (REs)**	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 (SCBs / CCBs), and any other entity which has been licensed 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) Asset Reconstruction Companies (ARCs) (e) All Payment System Providers (PSPs) / System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) (f) All authorised persons (APs), including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
32.	**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.

33.	**Suspicious Transaction**	means a 'transaction' as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith: (a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or (b) appears to be made in circumstances of unusual or unjustified complexity; or (c) appears to have no economic rationale or bona fide purpose; or (d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism. Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds that the Company suspects are 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.
34.	**Transaction**	means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes: a. opening of an account; b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means; c. the use of a safety deposit box or any other form of safe deposit; d. entering into any fiduciary relationship; e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or b) (f) establishing or creating a legal person or legal arrangement.
35.	**Video based Customer Identification Process (V-CIP)**	an alternative method by which an authorised official of the Company conducts customer identification with facial recognition and customer due diligence. This process involves a seamless, secure, live, informed- consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information which the customer furnished, through independent verification and by maintaining an audit trail of the process and the Company shall treat such processes complying with prescribed standards and procedures on par with face-to-face CIP for the purpose of these Directions.
36.	**Walk-in Customer**	means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.
37.	**Wire Transfer**	Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

CHAPTER – II: GENERAL

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

5. **Money Laundering and Terrorist Financing Risk Assessment:**

(1) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercises 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.
(2) 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 the Company from time to time.
(3) The Company shall properly document its risk assessment, and it shall be proportionate to the nature, size, geographical presence, complexity of activities / structure, etc. of the Company. Further, the Board or a committee of the Board to which it has delegated power shall determine the periodicity of the risk assessment exercise, in alignment with the outcome of the risk assessment exercise. However, the Company shall review it at least annually.
(4) The Company shall present the outcome of the exercise to the Board or any committee of the Board to which the Board has delegated power in this regard. The outcome shall also be made available to competent authorities and self-regulating bodies.

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

6. **Designated Director:**

(i) Designated Director means the Managing Director or a Whole-Time Director or Chief Executive Officer or any other Senior Officer 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.

7. **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.

8. **Compliance with KYC Policy:**

The Company shall ensure compliance with the KYC Policy through:

(i) The below-mentioned officials shall constitute as Senior Management and will be responsible for effective implementation of KYC policies and procedures:
- Managing Director / Chief Executive Officer
- National Credit & Operations Head
- Functional Departmental Heads

(ii) Allocating responsibilities through a Delegation of Powers Policy and Matrix for effective implementation of policies and procedures.

(iii) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements through the Internal Audit function.

(iv) 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.

(v) 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

9. **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 Company, under the guidelines in respect of Customer Acceptance, shall:

(1) not open any account in an anonymous or fictitious / benami name.
(2) open no account where it is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or unreliability 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.
(3) not undertake a transaction or an account-based relationship without following the CDD procedure.
(4) mandatory information to be sought for KYC purposes while opening an account and during the periodic updation.
(5) obtain additional information, where its internal KYC Policy has not specified such information requirement, with the explicit consent of the customer.
(6) apply the CDD procedure at the Unique Customer Identification Customer (UCIC) level. Thus, if an existing KYC-compliant customer of the Company desires to open another account or avail of any other product or service from the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
(7) follow the CDD Procedure for all the joint account holders, while opening a joint account.
(8) clearly spell out the circumstances in which a customer is permitted to act on behalf of another person / entity.
(9) put in place a suitable system 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 these Directions.
(10) verify the Permanent Account Number (PAN) (if obtained) from the verification facility of the issuing authority.
(11) verify the customer's digital signature on the equivalent e-document (if obtained) as per the provisions of the Information Technology Act, 2000 (21 of 2000).
(12) verify the Goods and Services Tax (GST) number from the search / verification facility of the issuing authority, where the GST details are available.
(13) SMHFC will also use RBI/ NHB caution advices in determining the customer acceptance framework.
(14) 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 including the Persons with Disabilities (PwDs). The Company shall not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned shall duly record the reason(s) for rejection.

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

10. **Risk Management:**

(i) 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) The Company shall undertake risk categorisation based on parameters such as the customer's identity, social / financial status, nature of business activity, and information about the customer's business and its location, geographical risk covering customers as well as transactions, type of products / services offered, delivery channel used for delivery of products / services, types of transactions undertaken such as cash, cheque / monetary instruments, wire transfers, forex transactions, etc. The Company may also factor in the ability to confirm identity documents through online or other services offered by issuing authorities, while considering customer's identity.

(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 may also use the FATF Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association (IBA), and other agencies, etc., in its risk assessment.

(v) The Company has in place a separate Policy viz. 'Policy on KYC Risk Categorisation' and the Risk Categorisation of customers shall be carried out as per the said Policy.

CHAPTER – V: CUSTOMER IDENTIFICATION PROCEDURE (CIP)

11. Customer Identification Procedure (CIP):

(i) The Company shall undertake identification of customers in the following cases:

(1) Commencement of an account-based relationship with the customer.
(2) Carrying out any international money transfer operations for a person who is not an account holder of the Company.
(3) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
(4) Selling third-party products as agents, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than ₹50,000.
(5) Carrying out transactions for a non-account-based customer, i.e., a walk-in customer, where the amount involved is equal to or exceeds ₹50,000 whether conducted as a single transaction or several transactions that appear to be connected.
(6) 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 ₹50,000.
(7) The Company shall ensure it does not seek introductions 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:

12. **Part I - 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:

(1) the Aadhaar number where,

(i) they are desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
(ii) they decide to submit their Aadhaar number voluntarily to the Company.

(2) the proof of possession of Aadhaar number where the Company can carry out offline verification; or

(3) the proof of possession of Aadhaar number where the Company cannot carry out the offline verification or any OVD or the equivalent e-document thereof containing the details of their identity and address; or

(4) the KYC Identifier with explicit consent to download records from CKYCR; and

(5) the Permanent Account Number (PAN) or the equivalent e-document thereof or Form No. 97 as defined in Income-tax Rules, 2026; and

(6) the Company may require 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 as per the Credit Policy of the Company.

Provided that where the customer has submitted,

(i) Aadhaar number under clause (1) above to a Company notified under first proviso to sub-section (1) of section 11A of the PML Act, such Company shall carry out authentication of the customer's Aadhaar number using UIDAI's e-KYC authentication. Further, in such a case, if the customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, they may give a self-declaration to that effect to the Company.

(ii) proof of possession of Aadhaar under clause (2) above where offline verification can be carried out, the Company shall carry out offline verification.

(iii) 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 issued thereunder and take a live photo as specified under Annexure D below.

(iv) any OVD or proof of possession of Aadhaar number under clause (3) above where offline verification cannot be carried out, the Company shall carry out verification through Digital KYC as specified under Annexure D below.

(v) KYC Identifier under clause (4) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with Clause 33 of this Policy.

Provided that for a period not beyond such date as the Government may notify for a class of REs, instead of carrying out digital KYC, the Company pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where the customer does not submit an equivalent e- document.

Provided further that in case the Company cannot perform an e-KYC authentication for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. An official of the Company shall invariably carry out CDD done in this manner, and such exception handling shall also be a part of the internal audit as mandated in Clause 8 of this Policy. The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The Company shall subject the database to periodic internal audit / inspection and the Company shall make database available for supervisory review.

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

Explanation 2: The Company official can perform biometric-based e-KYC authentication, including Aadhaar Face Authentication.

Explanation 3: The Company shall ensure that the use of Aadhaar, proof of possession of Aadhaar etc., is in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Explanation 4: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016), the customer shall provide the Aadhaar number to the Company. In other cases, customers may provide the Aadhaar number voluntarily.

(ii) **Simplified procedure for opening accounts by NBFCs**: In case a person who desires to open an account is not able to produce documents, as specified in Clause 12, the Company may, at their discretion, open accounts subject to the following conditions:

(i) The Company shall obtain a self-attested photograph from the customer.

(ii) The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(iii) The account shall remain operational initially for a period of twelve months, within which CDD as per Clause 12 and 13 of this Policy shall be carried out.

(iv) Balances in all their accounts taken together shall not exceed ₹50,000 at any point of time.

(v) The total credit in all the accounts taken together shall not exceed Rupees One Lakh in a year.

(vi) The Company shall make customer aware that no further transactions will be permitted until the full KYC procedure is completed in case directions (iv) and (v) above are breached by him.

(vii) The Company shall notify the customer when the balance reaches ₹40,000 or the total credit in a year reaches ₹80,000 that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in directions (iv) and (v) above.

(viii) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per Clause 12 and 13 of this Policy.

(iii) KYC verification once done by one branch / office of the Company shall be valid for transfer of the account to any other branch / office of the Company, provided the Company has already completed the full KYC verification for the concerned account and the same is not due for periodic updation.

(iv) **Video Customer Identification Process (V-CIP)**

The Company may undertake V-CIP to carry out:

(1) CDD in case of new customers onboarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

(2) Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Paragraph 31 and Paragraph 32 of the Directions, apart from undertaking CDD of the proprietor.

(3) Conversion of existing accounts opened in non-face-to-face mode using Aadhaar OTP based e-KYC authentication as per Clause 12 (v) of this Policy.

(4) Updation / Periodic updation of KYC for eligible customers.

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

(v) **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 be subject to the following conditions:

(1) The Customer shall give specific consent for the authentication through OTP.

(2) As a risk-mitigating measure for such accounts, the Company shall ensure that it sends transaction alerts, OTP, etc., only to the mobile number of the customer registered with Aadhaar.

The Company shall have a Board-approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

(3) The aggregate balance of all the deposit accounts of the customer shall not exceed Rupees One Lakh. In case the balance exceeds the threshold, the Company shall cease the account's operation, until it completes the CDD as mentioned at (6) below.

(4) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed Rupees Two Lakh.

(5) As regards borrowal accounts, the Company shall sanction only term loans. The aggregate amount of term loans sanctioned shall not exceed ₹60,000 in a year.

(6) The Company shall not allow accounts, both deposit and borrowal, opened using OTP based e-KYC to operate for more than one year unless it carries out identification as per Clause 12 of this Policy or as per V-CIP. If the Company uses Aadhaar details as per V-CIP it shall follow the process in its entirety, including fresh Aadhaar OTP authentication.

(7) If the Company does not complete the CDD procedure as mentioned above within a year; (a) in respect of deposit accounts, the Company shall close the same immediately, and (b) in respect of borrowal accounts, the Company shall allow no further debits.

(8) The Company shall obtain declaration from the customer to the effect that no other account has been opened nor will be opened using OTP-based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face- to-face mode.

(9) The Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above-mentioned conditions.

13. Part II - Customer Due Diligence (CDD) Measures for Sole Proprietary firms and Legal Entities shall be in accordance with Chapter VI (B) and (C) of the RBI Master Directions.

14. Part III - Customer Due Diligence (CDD) Measures for Identification of Beneficial Owner (BO):

For opening an account of a Legal Person who is not a natural person, the Company shall identify the beneficial owner(s) and shall undertake all reasonable steps in terms of sub- rule (3) of Rule 9 of the Rules to verify their identity, keeping in view the following:

(1) Where the customer or the owner of the controlling interest is:

(i) an entity listed on a stock exchange in India, or

(ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

(iii)it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

(2) In cases of trust / nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. In such cases, the

Company shall obtain satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.

15. **Ongoing Due Diligence:**

1. The Company shall undertake ongoing due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

2. Without prejudice to the generality of factors that call for close monitoring, the Company shall necessarily monitor the following types of transactions:

   a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
   b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
   c) High account turnover inconsistent with the size of the balance maintained.
   d) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

   For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI and ML) technologies to support effective monitoring.

3. For the purpose of risk categorization, the Company has put in place a separate Board approved Policy named "Policy for KYC Risk Categorisation".

4. The Company shall align the extent of monitoring with the risk category of the customer.

   a) The Company has put in place a system of periodic review of risk categorisation of accounts, with such periodicity being **at least once in every six months** and shall establish the need for applying enhanced due diligence measures.
   b) The Company shall closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) companies.

   Explanation: The Company shall subject high-risk accounts to more intensified monitoring.

5. **Updation / Periodic Updation of KYC:**

(ix) The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, the Company shall carry out periodic updation **at least once in every two years for high-risk customers**, **once in every eight years for medium risk customers** and **once in every 10 years for low-risk customers** from the date of opening of the account / last KYC updation.

(x) Notwithstanding the provisions given above, in respect of an individual customer who is categorised as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or up to June 30, 2026, whichever is later. The Company shall subject accounts of such customers to regular monitoring. This shall also apply to low-risk individual customers for whom periodic updation of KYC has already fallen due.

(xi) **Individuals:**

a) No change in KYC information: In case of no change in the KYC information, the Company shall obtain a self-declaration from the customer in this regard through the customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (including mobile application of Company) letter, etc.

b) Change in address: In case of a change only in the address details of the customer, the Company shall obtain a self-declaration of the new address from the customer through customer's email-id registered with the NBFC, customer's mobile number registered with the NBFC, ATMs, digital channels (including mobile application of NBFC), letter, etc., and shall verify the declared address through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

c) Further, the Company at its option, may obtain a copy of OVD or deemed OVD, as defined in Clause 3(24) or the equivalent e-documents thereof, as defined in Clause 3(16) of this Policy for the purpose of proof of address, declared by the customer at the time of updation / periodic updation. However, the Company shall clearly specify such requirement, in its internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

d) Accounts of customers, who were minor at the time of opening account, on their becoming major: In case of customers for whom the Company opened an account when they were minors, the Company shall obtain fresh photographs upon their becoming a major and, at that time, shall ensure that CDD documents as per the current CDD standards are available. Wherever required, the company may carry out fresh KYC of such customers, i.e., customers for whom it opened account when they were minor, upon their becoming a major.

e) The Company may use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation. To clarify, conditions stipulated in Clause 12(iv) of this Policy are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

f) Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

(xii) **Customers other than Individuals:**

(i) No change in KYC information: In case of no change in the KYC information of the LE customer, the Company shall obtain a self-declaration in this regard from the LE customer through its email id registered with the Company, ATMs, digital channels (including mobile application of Company), letter from an official authorised by the LE in this regard, board resolution, etc. Further, the

Company 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, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

(xiii) **Additional measures:** In addition to the above, the Company shall ensure that,

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

(ii) The Company verifies the Customer's PAN details, if available, from the database of the issuing authority at the time of periodic updation of KYC.

(iii) The Company provides an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, the Company shall ensure that it promptly updates the information / documents obtained from the customers at the time of updation / periodic updation of KYC in its records / database and provide an intimation, mentioning the date of updation of KYC details, to the customer.

(iv) In order to ensure customer convenience, the Company may consider making available the facility of updation / periodic updation of KYC at any branch.

(v) The Company shall adopt a risk-based approach with respect to periodic updation of KYC. For the purpose of risk categorization, the Company has put in place a separate document named "Policy for KYC Risk Categorisation". The Company has clearly specified in its internal policy, duly approved by the Board of Directors, any additional and exceptional measures, it adopts that are not otherwise mandated under this Policy.

(xiv) 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 the Company's end.

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

of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation / reminder may, inter alia, contain easy-to-understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation / reminder shall be duly recorded in the Company's system against each customer for audit trail.

6. In case of existing customers, the Company shall obtain the PAN or equivalent e-document thereof or Form No. 97, by such date which the Central Government may notify, failing which the Company shall temporarily cease operations in the account until the customer submits the PAN or equivalent e-documents thereof or Form No. 97.

Provided that before temporarily ceasing operations for an account, the Company 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.97 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 a Company gives in writing to the Company that they do not want to submit their PAN or equivalent e-document thereof or Form No. 97, the Company 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 paragraph, '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 the Company till such time the customer complies with the provisions of this paragraph. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

16. **Enhanced Due Diligence Procedure:**

(i) **Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Clause 12 (v)):**
Non-face-to-face onboarding facilitates a Company to establish a relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph include 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.

Currently, the Company does not open accounts through non-face-to-face mode. However, in future if the Company decides to open accounts using such mode, the following EDD measures shall be undertaken by company for non- face-to- face customer onboarding:

a. If the Company has introduced the process of V-CIP, it shall provide the same as the first option to the customer for remote onboarding. The Company shall treat processes complying with prescribed standards and procedures for V-CIP on par with face-to-face CIP for the purpose of this Policy.
b. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. The Company shall permit transactions only from the mobile number used for account opening.
c. Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. The Company may carry out the positive confirmation by means of such as address verification letter, Company point verification, deliverables, etc.
d. The 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. The Company shall categorise such customers as high-risk customers and shall subject accounts opened in non-face-to-face mode to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.
The guidelines for carrying our 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) The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP.
b) Reasonable measures shall be 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

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

(iii) **Customer Accounts Opened by Professional Intermediaries:**

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

a. The Company shall identify clients when a professional intermediary opens a client account on behalf of a single client.
b. The Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c. The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality which prohibits disclosure of client details to the Company.
d. The Company shall identify all the beneficial owners where intermediaries do not co-mingle funds at the level of the Company, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the Company, the Company shall look for beneficial owners.
e. The Company shall, at their 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.
f. The ultimate responsibility for knowing the customer lies with the Company.

CHAPTER - VII: RECORD MANAGEMENT

17. The Company shall take the following steps regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. The Company shall,

(1) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;
(2) preserve the records pertaining to the identification of the customers and their addresses, obtained while opening the account and during the course of business relationship, for at least five years after the business relationship has ended;
(3) swiftly make available, the identification records and transaction data to the competent authorities upon request;
(4) introduce a system of maintaining proper records of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
(5) maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit the reconstruction of an individual transaction, including the following:
    (i) the nature of the transactions;
    (ii) the amount of the transaction and the currency in which it was denominated;
    (iii) the date on which the transaction was conducted; and
    (iv) the parties to the transaction.
(6) evolve a system for proper maintenance and preservation of account information in a manner that allows the Company to retrieve data easily and quickly whenever required or when competent authorities request it;
(7) maintain records of the identity and address of its customers, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation: For the purpose of this paragraph, 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.

18. The Company shall ensure that in case of customers who are non-profit organisations, the Company registers details of such customers on the DARPAN Portal of NITI Aayog. If they are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

CHAPTER VIII: REPORTING REQUIREMENTS

19. The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in accordance with Rule 7 thereof.

    Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.
20. The Company shall take note of the reporting formats and comprehensive reporting format guide, prescribed / released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports. The Company which is yet to install / adopt suitable technological tools for extracting CTR / STR from its live transaction data shall make use of the editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU- IND has placed on its website. The Principal Officer of the Company, shall have suitable arrangement to cull out the transaction details from branches which are yet to be computerised and to feed the data into an electronic file with the help of the editable electronic utilities of CTR / STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

21. When furnishing information to the Director, FIU-IND, a delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute as a separate violation. The Company shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

22. 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 paragraph 8 of the Directions of any analysis of transactions and activities which appear unusual, if the Company has done any such analysis.

23. To identify and report suspicious transactions effectively, the Company shall implement robust software that generates alerts when transactions are inconsistent with a customer's risk categorisation and updated profile.

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

CHAPTER IX: REQUIREMENTS / OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES

24. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(1) The Company shall ensure that in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does 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', established and maintained pursuant to Security Council resolutions 1267 / 1989 / 2253, which includes names of individuals and entities associated with Al-Qaida, is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

(ii) The 'Taliban Sanctions List', established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://www.un.org/securitycouncil/sanctions/1988/materials

(2) The Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The Company shall verify the aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, on a daily basis, and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

(3) The Company shall report the details of accounts resembling any of the individuals / entities in the lists to FIU-IND in addition to advising the Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 (Annex I of the Directions).

(4) Freezing of Assets under section 51A of UAPA, 1967: The Company shall strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 (Annex I of the Directions), and shall ensure the meticulous compliance with the Order issued by the Government. The list of Nodal Officers for UAPA is available on the website of MHA.

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

(1) The 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 1, 2023, by the Ministry of Finance, Government of India (Annex II of the Directions).

(2) In accordance with paragraph 3 of the aforementioned Order, 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.

(3) Further, 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 Company account, etc.

(4) In case of a match in the above cases, the 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. The Company shall send a copy of the communication to the State Nodal Officer, where the account / transaction is held and to the RBI.

(5) The Company notes that, in terms of paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(6) The Company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(7) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, 2005, the Company shall prevent such individual / entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

(8) In case the Company receives an order to freeze assets under section 12A from the CNO, the Company shall , without delay, take necessary action to comply with the Order.

(9) The Company shall observe the process of unfreezing of funds, etc., as per paragraph 7 of the Order. Accordingly, the Company shall forward a copy of application received from an individual / entity regarding unfreezing, 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.

26. The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, 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.

27. In addition to the above, the Company shall take into account:

(1) other UNSCRs; and

(2) 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.

28. The Company shall undertake countermeasures when called upon so to do by any international or intergovernmental organisation of which India is a member and which is accepted by the Central Government.

29. **Jurisdictions that do not or insufficiently apply the FATF Recommendations:**

a) The Company shall consider the FATF Statements circulated by the RBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations. The 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) The Company shall give special attention 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 processes referred to in (1) and (2) above do not preclude the Company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

c) The Company shall examine 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, retain written findings together with all documents, and make them available to the RBI / other relevant authorities, on request.

30. The Company will leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

CHAPTER – X: OTHER INSTRUCTIONS

31. **Secrecy Obligations and Sharing of Information:**

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

32. **Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010:** The Company shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010, and Rules made thereunder. Further, the Company shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the RBI based on advice received from the Ministry of Home Affairs, Government of India.

33. **CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR):**

(1) In terms of provision of Rule 9(1A) of the PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
(2) Operational Guidelines for uploading the KYC data have been released by CERSAI.
(3) The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
(4) The 'live run' of the CKYCR started from July 15, 2016, in phased manner beginning with new 'individual accounts'. Company shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.
(5) The Company shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The Company shall upload KYC records as per the LE Template released by CERSAI.
(6) Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual / LE as the case may be.
(7) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload / update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (5) and (6), respectively, at the time of periodic updation as

specified in Clause 15.5 of this Policy, or earlier, when the updated KYC information is obtained / received from the customer. Also, whenever the Company obtains additional or updated information from any customer as per clause (10) below in this paragraph or Rule 9 (1C) of the PML Rules, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Company.

(8) The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(9) For the purpose of establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer 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; or
b. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
c. the validity period of downloaded documents has lapsed; or
d. the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

[Explanation: The RE that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, any Company downloading and relying on such records from the CKCYR shall not be required to re-verify the authenticity of the customer's identity and / or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. The Company downloading and relying on KYC records downloaded from the CKCYR shall remain responsible for all aspects of CDD procedure and provisions of these Directions, except verification of identity and / or address of the customer.]

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

Under FATCA and CRS, the Company shall adhere to the provisions of Income Tax Rules 238, 239 and 240 and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 240 and if so, shall take following steps for complying with the reporting requirements:

(1) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution.

(2) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 166 or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.
Explanation: Company shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 240.
(3) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 240.
(4) Develop a system of audit for the IT framework and compliance with Rules 238, 239 and 240 of Income Tax Rules, 2026.
(5) Constitute a 'High-Level Monitoring Committee' under the Designated Director or any other equivalent functionary to ensure compliance.
(6) 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 and available on the website http://www.incometaxindia.gov.in/Pages/default.aspx. REs may take note of the following:
(i) updated Guidance Note on FATCA and CRS; and
(ii) a press release on 'Closure of Financial Accounts' under Rule 240 (8).

35. **Operation of accounts and Money Mules:** The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to accounts by recruiting third parties which act as "money mules." The Company shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the concerned NBFC, it shall then be deemed that the Company has not complied with the Directions.

36. The Company shall allot Unique Customer Identification Code (UCIC) while entering new relationships with individual customers as also the existing individual customers.

37. The Company shall, at their option, not issue UCIC to all walk-in / occasional customers 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.

38. **Introduction of New Technologies –**

The Company shall identify and assess the ML / TF risks 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 existing products.

Further, the Company shall ensure:
(1) to undertake the ML / TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(2) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

39. Wire Transfer

(1) Information requirements for wire transfers for the purpose of this Policy:

(i) All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a. name of the originator;
b. the originator account number where such an account is used to process the transaction;
c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
d. name of the beneficiary; and
e. the beneficiary account number where such an account is used to process the transaction.

In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

(ii) In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

(iii) Domestic wire transfer, where the originator is an account holder of the ordering NBFC, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

(iv) Domestic wire transfers of ₹50,000 and above, where the originator is not an account holder of the ordering NBFC, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

Provided that in case of domestic wire transfers below ₹50,000 where the originator is not an account holder of the ordering Company and where the information accompanying the wire transfer can be made available to the beneficiary RE and appropriate authorities by other means, it is sufficient for the ordering Company to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

Provided further that the ordering Company shall make the information available within three working / business days of receiving the request from the intermediary RE, beneficiary RE, or from appropriate competent authorities.

(v) The Company shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting / competent authorities as well as FIU-IND on receiving such requests with appropriate level provisions.

(vi) The wire transfer instructions are not intended to cover the following types of payments:

(a) Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions, and the necessary information should be included in the message.

(b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated, financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact on the obligation of the Company to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

(2) Responsibilities of ordering NBFC, intermediary Company and beneficiary NBFC, effecting wire transfer, are as under:

(i) Ordering NBFC:

(a) The ordering Company shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per sub-clauses (iii) and (iv) of clause (1) above}, contain required and accurate originator information and required beneficiary information, as indicated above.

(b) Customer Identification shall be made if a customer, who is not an account holder of the ordering NBFC, is intentionally structuring domestic wire transfers below ₹50,000 to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.

(c) Ordering Company shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this paragraph.

(ii) Intermediary NBFC:

(a) The Company processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.

(b) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary Company shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary RE.

(c) Intermediary Company shall take reasonable measures to identify cross- border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.
(d) Intermediary Company shall have effective risk-based policies and procedures for determining:

- when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
- the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

(iii) Beneficiary NBFC:

(a) Beneficiary Company shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross- border wire transfers and qualifying domestic wire transfers {viz., transactions as per sub-clauses (iii) and (iv) of clause (1) above}, that lack required originator information or required beneficiary information.
(b) Beneficiary Company shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

(iv)Money Transfer Service Scheme (MTSS) providers and other NBFCs, shall comply with all of the relevant requirements of this paragraph, whether they are providing services directly or through their agents. The Company that control both the ordering and the beneficiary side of a wire transfer shall:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
(b) file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

(3) Other Obligations:

(i) Obligations in respect of the NBFC's engagement or involvement with unregulated entities in the process of wire transfer: The Company shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned Company shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that:
  (a) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
  (b) the agreement / arrangement, if any, with such unregulated entities by the Company clearly stipulates the obligations under wire transfer instructions; and
  (c) a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements,

the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

(ii) The Company's responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities). The Company is prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Directions, the Company shall ensure that they do not process cross-border transactions of designated persons and entities.

(iii) The Company's responsibility to fulfil record management requirements: Complete originator and beneficiary information relating to wire transfers shall be preserved by the Company involved in the wire transfer, in accordance with Clause 41 of this Policy.

40. **Quoting of PAN:**

PAN or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 159 applicable to NBFCs, as amended from time to time. Form 97 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

41. **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, it shall comply with the following aspects for the purpose of these directions:

(1) the identity and address of the walk-in customer shall be verified for transactions above ₹50,000 as required under Clause 11(i)(5) of this Policy.
(2) transaction details of sale of third-party products and related records shall be maintained as prescribed in Clause 17 of this Policy.
(3) 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.
(4) transactions involving ₹50,000 and above shall be undertaken only by:
    (i) debit to customers' account or against cheques; and
    (ii) obtaining and verifying the PAN given by the account-based as well as walk-in customers.
(5) Instruction at (4) above shall also apply to sale of the Company's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for ₹50,000 and above.

42. **Hiring of Employees and Employee training:**

(1) The Company shall put in place an adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of its personnel recruitment / hiring process.
(2) The Company 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. The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(3) The Company shall put in place an on-going employee training programme so that the members of staff are adequately trained in KYC / AML / CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The Company shall specially train the front desk staff to handle issues arising from lack of customer education. The Company shall ensure the proper staffing of the audit function with persons adequately trained and well-versed in KYC / AML / CFT policies of the NBFC, regulation and related issues.

43. **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 97 if PAN is not allotted

(3) **Certified Copy** * of one of the Officially Valid Documents (**OVD**s) listed below:

Sr. No.	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 in such form that the Unique Identification Authority of India (UIDAI) issues.**
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
v	Certificate / Registration document issued by Sales Tax / Service Tax / Professional Tax Authorities
vi	IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute
vii	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
viii	Utility Bills such as Electricity, Water, and Landline Telephone bills in the Name of the Proprietary Concern

In cases where the Company is satisfied that it is not possible to furnish two such documents, it may, at its discretion, accept only one of those documents as proof of business / activity.
Provided that the Company shall undertake a contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that it has verified the business activity from the address 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
iii	Registration Certificate
iv	GST/ CST/ VAT certificate (Provisional / Final)
v	Names of all the partners and any one KYC Documents for Individual mentioned in **Point A** of each partner
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.

(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
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.
Ix	Resolution from the Board of Directors or power of attorney granted to its managers, officers or employees to transact on its behalf.

(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 97 of the Trust
ii	Trust Deed
iii	Registration Certificate
iv	the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
v	the address of the registered office of the trust; and
vi	The names of 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. No.	Document Name
i	PAN or Form 97 of the unincorporated association or a body of individuals
ii	Resolution of the managing body of such association or body of individuals
iii	Power of attorney granted to transact on its behalf
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. No.	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 97 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

Indicative List of Licenses / Certificates Issued in the Name of the Proprietary Firm by any Professional Body Incorporated under a Statute	
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 empowered to do so.
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)

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

a) **V-CIP Infrastructure**

(i) The Company shall have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for NBFCs, as updated from time to time as well as other general guidelines on IT risks. The Company shall house the technology infrastructure on its own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall comply with relevant RBI guidelines. Where the Company uses a cloud deployment model, it shall ensure that ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and the cloud service provider or third-party technology provider assisting the V-CIP shall retain no data.

(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 Company shall record the customer consent in an auditable and alteration-proof manner.

(iii) The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings shall contain the live GPS co-ordinates (geo tagging) of the customer undertaking the V-CIP and date and 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 high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company.

Explanation: Making specific facial gestures, like blinking of eyes, smiling, frowning, etc. is not mandatory for liveness check. The Company shall take due cognizance of special needs, if any, of the customer during liveness check.

(vi) The Company may use appropriate artificial intelligence (AI) technology to ensure that the V-CIP is robust.

(vii) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the Company shall regularly update the technology infrastructure including application software as well as workflows. The Company shall report any detected case of forged identity through V-CIP as a cyber event under extant regulatory guidelines.

(viii) The Company shall subject the V-CIP infrastructure to necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. The Company shall mitigate any critical gap reported under this process before rolling out its implementation. The empaneled auditors of Indian Computer Emergency Response Team (CERT-In) shall conduct such tests. Such tests shall also be carried out periodically in conformance to internal / regulatory guidelines.

(ix) The Company shall subject the V-CIP application software and relevant APIs / webservices to appropriate testing of functional, performance, and maintenance strength before being used in live environment. The Company shall roll out the application only after closure of any critical gap found during such tests. 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 workflow 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 shall be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.

(ii) Disruption of any sort including pausing of video, reconnecting calls, etc., may not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then the Company may not initiate a fresh session. However, in case of call drop / disconnection, fresh session shall be initiated.

(iii) The Company shall vary the sequence and / or type of questions, including those indicating the liveness of the interaction, during video interactions to establish that the interactions are real-time and not pre-recorded.

(iv) The Company shall reject the account opening process if it observes any prompting at the customer end.

(v) The Company shall factor in the fact that the V-CIP customer is an existing or new customer, or if the case relates to one rejected earlier or if the name appears in some negative list, at an appropriate stage of workflow.

(vi) The authorised official of the Company performing the V-CIP shall record audio and video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:

a. OTP based Aadhaar e-KYC authentication.
b. Offline Verification of Aadhaar for identification.
c. KYC records downloaded from CKYCR, in accordance with Clause 33 of this Policy using the KYC identifier provided by the customer.
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

(vii) The Company shall ensure to redact or blackout the Aadhaar number in terms of Clause 12 of this Policy.

(viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the Company shall ensure that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

(ix) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that it undertakes video process of the V-CIP 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, the Company shall ensure that no incremental risk is added due to this.

(x) If the address of the customer is different from that indicated in the OVD, the Company shall capture suitable records of the current address, as per the existing requirement. The Company shall ensure that it also confirms the economic and financial profile / information submitted by the customer from the customer undertaking the V-CIP in a suitable manner.

(xi) The Company shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The Company shall verify the PAN details from the database of the issuing authority, including through DigiLocker.

(xii) The use of printed copy of equivalent e-document, including an e-PAN is not valid for the V-CIP.

(xiii) 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.

(xiv) The Company shall make all accounts opened through V-CIP operational only after subjecting them to concurrent audit to ensure the integrity of process and its acceptability of its outcome.

(xv) The Company shall appropriately comply with all matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act.

c) **V-CIP Records and Data Management**

(i) The Company shall store the entire data and recordings of V-CIP in a system / system 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 these directions, shall also apply to V-CIP.

(ii) The Company shall preserve the activity log along with the credentials of the official performing the V-CIP.

Annexure - D

Digital KYC Process

(1) The Company shall develop an application for digital KYC process and make it available at customer touch points for undertaking KYC of its customers and shall undertake the KYC process only through this authenticated application.

(2) The Company shall control the access to the Application and shall ensure that unauthorised persons do not use it. Authorised officials shall access the Application only through a login-id and password or a Live OTP or Time OTP controlled mechanism that the Company provides.

(3) The customer, for the purpose of KYC, shall visit the location of the authorised official of the Company or vice-versa. The original OVD shall be in possession of the customer.

(4) The Company shall ensure that the authorised officer takes a Live photograph of the customer and embeds the same photograph in the Customer Application Form (CAF). Further, the Company's system Application shall put a watermark in readable form, containing the CAF number, GPS coordinates, authorised official's name, unique employee code (which the Company assigns) and date (DD:MM: YYYY) and time stamp (HH:MM:SS), on the captured live photograph of the customer.

(5) The Company's Application shall have the feature that it captures only a live photograph of the customer and does not capture any printed or video graphed photograph. The background behind the customer while capturing live photograph shall be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

(6) Similarly, the authorised officer shall capture the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), vertically from above and shall apply a water-marking in readable form as mentioned above. The authorised officer shall ensure there is no skew or tilt in the mobile device while capturing the live photograph of the original documents.

(7) The authorised officer shall capture the live photograph of the customer and his original documents in proper light so that they are clearly readable and identifiable.

(8) Thereafter, the authorised officer shall fill all the entries in the CAF as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details may 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 may be auto-populated by scanning the QR available on Aadhaar / e-Aadhaar.

(9) 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, the Company will treat it as the customer's signature on CAF. However, if the customer does not have their own mobile number, the Company may use the mobile number of their family / relatives / known persons for this purpose and clearly mention it in the CAF. In any case, the Company shall not use the mobile number of authorised officer registered with the Company for the customer signature. The Company shall check that the mobile number used in customer signature is not the mobile number of the authorised officer.

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

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

(12) The authorised officer of the Company shall check and verify that:

(i) information available in the picture of the document matches with the information entered by authorised officer in CAF.

(ii) live photograph of the customer matches with the photo available in the document.; and

(iii) the authorised officer has properly filled all of the necessary details in CAF, including mandatory field.

(13) On Successful verification, the CAF shall be digitally signed by authorised officer of the Company 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