SATYA Micro Housing Finance Private Ltd

सर्वे भवन्तु सुखिनः

(Formerly known as Baid Housing Finance Private Limited)

KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML) POLICY

Version 2.0

PREFACE

SATYA Micro Housing Finance Private Limited (Formerly known as Baid Housing Finance Private Limited), hereinafter refer as "SMHFPL"/"Company") is a Private Limited Company incorporated under the provisions of the Companies Act, 1956 and registered as a Housing Finance Company ("HFC") with the National Housing Bank ("NHB").

With the shifting of regulation of HFCs from NHB to RBI, now Reserve Bank of India's ("RBI") vide their circular dated May 19, 2020 made Master Direction - Know Your Customer (KYC) Direction, 2016, applicable to all HFCs. Subsequently, RBI vide circular dated February 17, 2021 re-iterated applicability of the above Master Direction - Know Your Customer (KYC) Direction, 2016 in the Master Direction – Non-Banking Financial Company – Housing Finance Company (Reserve Bank) Directions, 2021.

Accordingly, this Policy earlier prepared in terms of the NHB's Guidelines on KYC & AML, and approved by the Board, is being reviewed in the context of the RBI's Master Direction - Know Your Customer (KYC) Direction, 2016, Prevention of Money Laundering Act -2002, Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and such other regulatory laws as may be applicable on HFCs.

BACKGROUND

The Prevention of Money Laundering Act (PMLA), 2002 came into effect from 1st July, 2005 through a Gazette of India notification. As per the PMLA, 2002 read with Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 including any amendment thereof (PMLR 2005) (PMLA 2002 and PMLR 2005 will together referred to as PMLA), the offence of Money Laundering is defined as: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."

The Reserve Bank of India (RBI) has issued revised set of comprehensive 'Know Your Customer' Guidelines to all Non-Banking Financial Companies (NBFCs), Miscellaneous Non-Banking Companies and Residuary Non-Banking Companies in the context of the recommendations made by Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) and advised all NBFCs to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on KYC and AML measures are formulated and put in place with the approval of their respective Boards. Compliance with these standards both by the banks/financial institutions, including HFCs, has become necessary for international financial relationships. The 'Know Your Customer' Guidelines issued by the National Housing Bank for HFCs have been drafted and issued in the above context.

1. Objectives

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

CHAPTER-I PRELIMINARY

Applicability

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

This Policy establishes minimum requirements for the Company to establish, implement, and maintain an AML Program that is reasonably designed to:

(a) Implement this Policy: and

(b) To ensure compliance with applicable AML laws, rules and regulations.

This Policy requires the Company and each Employee to:

- Protect the Company from being used for money laundering or funding terrorist activities;
- Conduct themselves in accordance with the highest ethical standards
- Comply with the letter and the spirit of applicable AML Laws, and the Company's AML Program and procedures;
- Be vigilant and escalate AML procedures in respect of individuals/entities who attempt to violate or avoid KYC /AML, procedures or this Policy; and
- Cooperate with AML-related law enforcement and regulatory agencies fully under applicable laws.
- Designate official for reporting purposes to Financial Intelligence Unit (FIU).

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

2. Definitions

In these Guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

1. **"Aadhaar number"** means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016,

henceforth the' Aadhaar Act';

2. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto;

3. **"Authentication"** means the process as defined under sub-section (c) of section 2 of the Aadhaar Act;

4. **"Beneficial Owner (BO)"** means

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 person, has/have a controlling ownership interest or who exercise control through other means.

Explanation - For the purpose of this sub-clause:

*(i) "**Controlling ownership interest**" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.*

*(ii) "**Control**" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.*

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, has/have ownership off entitlement to more than 15 per cent of capital or profits of the partnership.

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 off entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

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% or more interest in the trust and other natural person exercising ultimate effective control over trust through a chain of control or ownership.

5. **"Certified Copy"** means obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the

copy by the authorised officer of the Company as per the provisions contained in the Act.

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

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

6. **"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.

7. **"The Company"** means SATYA Micro Housing Finance Private Limited (Formerly known as Baid Housing Finance Private Limited) ("SMHFPL").

8. **"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.

9. **"Counterfeit Currency Transaction"** means all cash transactions, where forged or counterfeit Indian currency notes have been used as genuine. These cash transactions should also include transactions where forgery of valuable security or documents has taken place.

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

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

12. **"Designated Director"** means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

    a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors
    b) The name, designation and address of the Designated Director shall be communicated to the Financial Intelligence Unit-India (FIU-IND).

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

14. **"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 (as amended from time to time, including any statutory modification(s) or re-enactment(s) thereof, for the time being in force).

15. **"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.

16. **"Equivalent e-document"** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

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

17. **"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.

18. **"Non-profit organizations (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

19. **"Officially Valid Document (OVD)"** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

    a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India (UIDAI).

    b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents there of shall be deemed to be OVDs for the limited purpose of proof of address:

        i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

        ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above;

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

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

20. "**Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section -2 of the Aadhaar Act.

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

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

23. **"Person"** has the same meaning as defined in the Act and includes:

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not
f. every artificial juridical person, not falling within anyone of the above persons (a to e), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

24. **"Principal Officer"**

a) An official designated by the Board of Directors of the Company for overseeing and managing the KYC & AML policies and processes.

b) The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
c) The name, designation and address of the Principal Officer shall be communicated to the Financial Intelligence Unit-India FIU-IND.

25. **"Senior Management"** - for the purpose of KYC compliance shall include members of the Management Committee, Designated Director, Head of Compliance, Principal Officer (PO) and his supervisor.

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

27. **"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;
f. establishing or creating a legal person or legal arrangement.

28. **"Video based Customer Identification Process (V-CIP)"** means a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

29. **"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.

30. **"Walk-in Customer"** means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.

31. **"Customer identification"** means undertaking the process of CDD.

32. **"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.

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

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

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

36. **"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.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER- II KNOW YOUR CUSTOMER STANDARDS

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The KYC policy of the Company includes the following four key elements:

(i) Customer Acceptance Policy;
(ii) Risk management.
(iii) Customer Identification Procedures;
(iv) Monitoring of Transactions

Money Laundering and Terrorist Financing Risk Assessment

- The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and

terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. as applicable from time to time.

- 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.
- The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.
- The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them If necessary.

Designated Director

Mr. Vivek Tiwari, Managing Director of the Company has been appointed as "Designated Director" to ensure overall compliance with the obligations imposed under Chapter IV of the Act.

Appointment of Principal Officer

The Company has appointed Mr. Ranjeet Kumar Mishra, Chief Executive Officer of the Company to be designated as ‘Principal Officer'. The Principal Officer will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, other HFC’s and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

Compliance of KYC Policy

The Company will ensure time to time compliance with KYC Policy through:

a. Allocation of responsibility for effective implementation of policies and procedures.
b. Independent evaluation of the compliance functions of HFC policies and procedures, including legal and regulatory requirements.
c. concurrent/internal audit system to verify the compliance with KYC/Anti-Money Laundering (AML) policies and procedures;

The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER -III CUSTOMER ACCEPTANCE POLICY (CAP)

Customer Acceptance Policy of the Company lays down explicit criteria for acceptance of customers, which ensures the following aspects of the customer relationship:

d. No account is opened in anonymous or fictitious/benami name(s);

e. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non- cooperation of the customer or non-reliability of the documents/information furnished by the customer.

f. No transaction or account based relationship is undertaken without following the CDD procedure.

g. The mandatory information to be sought for KYC purpose while opening an account and during the periodic Updation, is specified.

h. Additional information, is obtained with the explicit consent of the customer, where such information requirement is not mentioned in this policy.

i. The Company shall ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. For this purpose, the Company shall maintain lists of individuals or entities issued by Reserve Bank of India (RBI), United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/entities in the list shall be treated as suspicious and reported.

j. Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate due diligence.

k. The Company may rely on third party verification subject to the conditions prescribed by Reserve Bank of India (RBI) in this regard.

l. The information collected from the customer shall be kept confidential.

m. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision.

n. Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

Adoption of Customer Acceptance Policy of the Company and its implementation would not result in denial of the Company's services to general public, especially to those, who are financially or socially disadvantaged. In case of opening of any account of Politically Exposed Persons (PEP) necessary approvals from the Managing Director/ National Credit Head would be taken.

CHAPTER-IV RISK MANAGEMENT

The Board of Directors of the Company shall ensure that an effective KYC program is in place and by establishing appropriate procedures and is overseeing its effective implementation. The program shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated within the Company to ensure that The Company's policies and procedures are implemented effectively.

The Board of the Company will be updated from time to time about all customers of the Company having low risk profile given in the nature of its business, unless belonging to a higher risk profile listed above and approved as an exception. The Company shall apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

Given the nature of the business of the Company – small ticket loans to low income financially excluded families have categorized as low risk customers. It is highly unlikely that the Company will have any medium / high risk clients given its focus on the lower income section of society, but for information, examples of customers requiring higher due diligence may include:

(i) Non-resident customers,
(ii) High net worth individuals,
(iii) trusts, charities, NGOs and organizations receiving donations,
(iv) companies having close family shareholding or beneficial ownership,
(v) Firms with 'sleeping partners',
(vi) Politically exposed persons (PEPs) of foreign origin,
(vii) non-face to face customers, and
(viii) Those with dubious reputation as per public information available, etc.

The Recommendations made by the Financial Action Task Force (FATF) on Anti-money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards would also be used in risk assessment.

The Company has ensured that an effective KYC program is in place and has established appropriate procedures and is overseeing its effective implementation. The program covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Front line staff, both sales & operations, and credit staff of the Company are aware that no loan accounts

will be created unless the KYC procedures are adhered to completely.

Risk Categorization of Customers

Customers shall be categorised as Low, Medium and High-Risk category, based on the assessment and risk perception of the Company. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.. The Company will apply enhanced due diligence measures on high-risk customers, thereby conducting intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

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

The extent of monitoring shall be aligned with the risk category of the customer. KYC risk of the customers will be annually reviewed & presented before the Board of Directors of the Company.

For risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, are categorized as low risk.

Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments & Government owned companies, regulators and statutory bodies, etc.
Examples of customers requiring higher due diligence may include

- non-resident customers,
- high net worth individuals,
- trusts, charities, NGOs and organizations receiving donations,
- companies having close family shareholding or beneficial ownership,
- firms with 'sleeping partners',
- politically exposed persons (PEPs) of foreign origin,
- non-face to face customers, and
- those with dubious reputation as per public information available, etc.

As the Company is engaged in extending loans to households belonging to low / middle income group, the customers of Company are all classified as low risk, unless specifically identified in any other risk category. Thus, only the basic requirements of verifying the identity and location of the customer are to be met.

CHAPTER-V CUSTOMER IDENTIFICATION PROCEDURE (CIP)

The Company will follow clear NHB guidelines on the Customer Identification Procedure to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

The Company will undertake identification of customers in the following cases:

a. Commencement of an account-based relationship with the customer.
b. Carrying out any international money transfer operations for a person who is not an account holder of the Company.
c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
d. Selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.
e. carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
f. when the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
g. the Company shall ensure that introduction is not to be sought while opening accounts.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company shall at their option, rely on CDD done by a third party, subject to the following conditions:

(i) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
(ii) Adequate steps are taken by the Company 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.
(iii) 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 the Prevention of Money-Laundering Act.
(iv) The third party shall not be based in a country or jurisdiction assessed as high risk.
(v) The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the Company's discretion.

The Company may undertake live V-CIP, to be carried out by an official of the Company, for

establishment of an account-based relationship with an individual customer, after obtaining his informed consent:

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

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

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

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

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

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

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

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

ix) The activity log along with the credentials of the official performing the V-CIP shall be preserved and

x) The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xi) The Company shall ensure to redact or blackout the Aadhar Number obtained from the client.

CHAPTER- VI CUSTOMER DUE DILIGENCE (CDD)

Procedure:

Part- I CDD Procedure in case of individuals

Company shall apply the following procedure while establishing an account-based relationship with an individual or while dealing with the individual who is a beneficial owner, authorised signatory or the power

of attorney holder related to any legal entity:

(a) the Aadhaar number where:-
  (i) he/she desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act; or
  (ii) He/she decides to submit his Aadhaar number voluntarily to the company notified under first proviso to sub-section (1) of section 11A of the PML Act; or Such other documents pertaining to the nature of business or financial status specified by the Company in KYC policy / Norms.

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and
(ac) the KYC Identifier with an explicit consent to download records from CKYCR;

(b) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

(c) such other documents including in respect of the nature of business and financial status of the customer as may be required by the Company.

Provided that where the customer has submitted,

(i) Aadhaar number under clause (a) above to a Company notified under first proviso to sub-section (1) of section 11A of the Act, the company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he/she may give a self-declaration to that effect to the Company.
(ii) Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, 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 issues thereunder and take a live photo as specified under Annex I.
(iv) Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under Annex I.
(v) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a Company, 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 an equivalent

e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act 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.

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

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

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

Where the Company is suspicious 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.

Part- II CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, identification information as mentioned under Chapter IV in respect of the individual (proprietor) shall be obtained.

In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
(b) Certificate/license issued by the municipal authorities under Shop and Establishment Act.
(c) Sales and income tax returns.
(d) CST/VAT/GST certificate (provisional/ final).
(e) Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities.
(f) lEC (Importer Exporter Code) issued to the proprietary concern by the office of DCFT/License/ certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax

authorities.

(h) Utility bills such as electricity, water, and landline telephone bills.

In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/activity.

Provided that the Company shall undertake contact, point verification and collect such other information and clarification as may be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part- III CDD Measures for Legal Entities

For opening an **account of a company**, one certified copy of each of the following documents shall be obtained:

(a) Certificate of incorporation;
(b) Memorandum and Articles of Association;
(c) Permanent Account Number of the company;
(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
(e) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
(f) the names of the relevant persons holding senior management position; and
(g) the registered office and the principal place of its business, if it is different

For opening an account of a **partnership firm,** one certified copy of each of the following documents shall be obtained:

(a) Registration certificate;
(b) Partnership deed;
(c) Permanent Account Number of the partnership firm;
(d) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(e) the names of all the partners and
(f) address of the registered office, and the principal place of its business, if it is different.

For opening an account of a **TRUST**, one certified copy of each of the following documents shall be obtained:

(a) Registration certificate;
(b) Trust deed;
(c) Permanent Account Number or Form No.60 of the trust;
(d) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(e) the names of the beneficiaries, trustees, settlor and authors of the trust
(f) the address of the registered office of the trust; and
(g) list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

For opening an account of an **unincorporated association or a body of individuals**, one certified copy of each of the following documents shall be obtained:

(a) Resolution of the managing body of such association or body of individuals;
Permanent Account Number or Form No.60 of the unincorporated association or a body of individuals;
(b) Power of attorney granted to transact on its behalf;
(c) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
(d) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals..

Explanation - Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals, includes societies.

For opening accounts of **juridical persons** not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents shall be obtained:

(a) Document showing name of the person authorised to act on behalf of the entity;
(b) Aadhaar/PAN/ OVD for proof of identity and address in respect of the person holding an attorney to transact on its behalf and
(c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Part-IV CDD Measures for Identification of Beneficial Owner

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

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

Accounts of Politically Exposed Persons (PEPs):

(i) The Company can have the option of establishing a relationship with PEPs provided that:
(a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
(b) the identity of the person is verified before accepting the PEP
(c) The decision to open an account for a PEP is approved by National Credit head or MD/CEO
(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;

(f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

(ii) These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

Customer's accounts opened by Professional Intermediaries:

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

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

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

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

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

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

CHAPTER – VII ONGOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC procedures. The Company shall effectively control and reduce risk only if there is an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

(a) The Company will ensure special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

(b) The extent of monitoring will be aligned with the risk category of the customer. A system of periodic review of risk categorisation of accounts, with such periodicity as specified in this Policy shall be put in place.

(c) For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of two risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments & Government owned companies, regulators and statutory bodies, etc. In

such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met.

(d) Customers that are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. The Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include

- non-resident customers,
- high net worth individuals,
- trusts, charities, NGOs and organizations receiving donations,
- companies having close family shareholding or beneficial ownership,
- firms with 'sleeping partners',
- politically exposed persons (PEPs)of foreign origin,
- non-face to face customers, and
- those with dubious reputation as per public information available, etc.

Periodic Updation

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

CHAPTER – VIII MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of effective KYC procedures. The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

Maintenance of records of transactions:

(a) The Company shall introduce a system of maintaining proper record of transactions required under Prevention of Money Laundering Act (PMLA) as mentioned below:
   a) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions.
   b) All suspicious transactions whether or not made in cash.
   c) Records pertaining to identification of the customer and his/her address; and
   d) Should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

(b) The Company shall maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions so as to permit reconstruction of individual transactions, including the following:

(a) the nature of the transactions;
(b) the amount of the transaction and the currency in which it was denominated;
(c) the date on which the transaction was conducted; and
(d) the parties to the transaction.

Furnishing of information to the Director, Financial Intelligence Unit - India (FIU-IND)

In terms of the provisions of the Rule 8 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. The Company shall, inter-alia, furnish to the Director, FIU-IND

a) **Cash transaction report (CTR)/Counterfeit Currency Report (CCR)** - All such cash transactions where forged or counterfeit Indian currency notes of bank notes have been used as genuine as Counterfeit Currency Report (CCR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.

b) **Suspicious Transactions Reporting (STR)**- The Company shall endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to Financial Intelligence Unit-India (FIU-IND).

The Company shall file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

A copy of information furnished will be retained by the 'Principal Officer' for the purposes of official record.

- **Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports-**

The Company shall maintain utmost confidentiality in investigating suspicious activities and while reporting Counterfeit Currency Report (CCR)/ Suspicious Transactions Report (STR) to the Financial Intelligence Unit-India (FIU-IND)/ higher authorities. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

Prohibited List of Individuals/Entities:

The Company shall ensure that in terms of Section 51A of Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, any of the existing or new customers are not in the prohibited list of individuals and entities which are periodically prescribed by local regulator from time to time. Compliance monitoring of such individuals / entities are done periodically be screening them against the below lists provided under RBI Directions, as amended from time to time:

a. The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at https://scsanctions.un.org/ohz5jen-al-qaida.html.
b. The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/3ppp1en-taliban.htm. .

Pursuant to the above screening, if any of the accounts of customers of individuals or entities are categorised as 'High-Risk', then the Company shall follow the enhanced due diligence procedures prescribed under RBI Directions.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

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

The procedure laid down in the UAPA Order dated February 2, 2021, shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. Jurisdictions that do not or insufficiently apply the FATF Recommendations.

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

(i) Under FATCA and CRS, The Company adheres to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a reporting financial Institution as defined in Income Tax Rule 114F and if so, following steps would be taken for complying with the reporting requirements:

(a) Register on the related e-filling 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

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.
Explanation – spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://wwwfedai.org.in/ RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules will be referred.

(c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.

(d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(e) A "High Level Monitoring Committee" (Credit Committee) under the Designated Director to

ensure compliance as and when required.

(f) 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. Company may take note of the following:

i. updated Guidance note on FATCA and CRS

ii. a press release on 'Closure of Financial Accounts' under Rule 114H(8) of Income Tax Rules.

CHAPTER-VIII OTHER MEASURES

Secrecy Obligations and Sharing of Information

(i) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.

(ii) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(iii) While considering the requests for data/information from Government and other agencies, the Company shall satisfy that the information being sought is not of such a nature as shall violate the provisions of the laws relating to secrecy in transactions.

(iv) the exceptions to the said rule shall be as under:

a. Where disclosure is under compulsion of law
b. Where there is a duty to the public to disclose,
c. the interest of bank requires disclosure and
d. Where the disclosure is made with the express or implied consent of the customer.

Sharing KYC information with Central KYC Records Registry (CKYCR)

a. 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 as per the Operational Guidelines for uploading the KYC data issued CERSAI.

b. The Company shall capture the KYC information for sharing with the Central KYC Records Registry (C-KYCR) in the manner as prescribed in the Rules as per the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company shall upload the KYC data pertaining to all types of prescribed accounts with Central KYC Records Registry (CKYCR), as and when required, in terms of the provisions of the Rules.

Independent Evaluation

To provide reasonable assurance that its KYC and AML procedures are functioning effectively, an audit of its KYC and AML processes will covered under Internal Audit of the Company. The audit findings and compliance thereof will be put up before the Audit Committee of the Board.

Responsibilities of Senior Management

- **Designated Director**- The Company shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the Act and the Rules thereunder. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director".
- **Principal Officer**- An official (having knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business) shall be designated as the Principal Officer of the Company. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

Key Responsibilities of the Senior Management

a) Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under Act and Rules.

b) Proper implementation of the company's KYC & AML policy and procedures.

Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process is put in place.

(b) 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.

(c) On-going employee training programme shall be put in place 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 front desk staff will be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.

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

Annex I

Digital KYC Process

a. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.
b. The access of the Application shall be controlled by the Company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Company to its authorized officials.
c. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
d. The Company must ensure that the live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
e. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
f. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
g. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
h. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
i. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with OTP which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
j. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The authorized officer

shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

k. The authorized officer of the Company shall check and verify that information available in the picture of document is matching with the information entered by authorized officer in CAF:

(i) Live photograph of the customer matches with the photo available in the document; and

(ii) All of the necessary details in CAF including mandatory field are filled properly;

l. On Successful verification, the CAF shall be digitally signed by authorized 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.