India Housing Finance Pvt Ltd

KNOW YOU CUSTOMER AND ANTI MONEY LAUNDERING POLICY

Document Title	**Know Your Customer and Anti Money Laundering Policy**
Approved by	**Board of Directors**
Policy Owner	**Mr. Satish Bansal & Mr. Amit Srivastava (Risk & Operations Department)**
Date of Review/ Approval	**February 12, 2024**
Version No.	**1.0/ 2023-24**

KNOW YOUR CUSTOMER AND ANTI MONEY LAUNDERING POLICY

SECTION A: BACKGROUND, OBJECTIVES AND APPLICABILITY

1 Background

The Government of India has enacted and notified the 'Prevention of Money Laundering Act, 2002' ("**PMLA**") to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto. Further, under the PMLA, the 'Prevention of Money-Laundering (Maintenance of Records Rules), 2005' ("**PML Rules**") have been notified for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the reporting entities.

Based on the PMLA and PML Rules, the Reserve Bank of India ("**RBI**") has prescribed the Reserve Bank of India {Know Your Customer (KYC)} Directions, 2016 ("**RBI KYC Directions**"), provisions of which are required to be complied by various types of entities regulated by RBI. The RBI KYC Directions have prescribed guidance on various operational aspects relating to the same and, in this regard, advised that a regulated entity should adopt a policy duly approved by its Board of Directors ("Board") or any committee of the Board to which power may be delegated.

Accordingly, **AVIOM India Housing Finance Private Limited**, as Housing Finance Company ("**HFC**") is required to comply with various applicable provisions of the PMLA, PML Rules and the RBI KYC Directions.

2 Scope and Objectives of the KYC & AML Policy

2.1 In accordance with the latest RBI KYC Directions, AVIOM India Housing Finance Private Limited ("**Company**") has reviewed its existing 'Know Your Customer ("**KYC**") and Anti-Money Laundering ("**AML**") Policy ("**KYC & AML Policy**" or "**Policy"**). Once approved by the Board of Directors of the Company ("**Board**"), this version of the Policy shall supersede all prior versions of the KYC and AML Policy adopted by the Company.

2.2 The KYC & AML Policy covers the following 4 key elements:

(a) To lay down the criteria for Customer Acceptance Policy ("**CAP**");

(b) Risk Management from Money Laundering Risk perspectives;

(c) To lay down criteria for Customer Identification Procedures ("**CIP**"); and

(d) To establish procedures for monitoring of transactions.

2.3 The objectives of the Policy are as under:

(a) To prevent the Company from being used, intentionally or un-intentionally, by criminal elements for money laundering activities.

(b) To know/understand the customers and their financial dealings better, which in turn, help in managing their risks prudently.

3 Applicability

This KYC and AML Policy shall be applicable to all customers of the Company, which for the purposes of this Policy shall mean persons who are 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.

All the officials, representatives, and any third parties engaged by the Company to perform any of the requirements prescribed under the RBI KYC Directions, shall be required to ensure compliance with the provisions of this Policy.

4 Approval Authority and Review of the Policy

The Policy shall require approval of the Board. It shall be placed before the Board at least once in a year if not earlier required by the RBI KYC Directions or any other regulatory/ supervisory directions. Any review/ amendment in the Policy shall be recommended by the Risk Management Committee to the Board for its approval. However, if there are any amendments in the Policy which are necessitated due to any regulatory requirement/ amendment then the same may be done after approval from the Designated Director based on the recommendation of the Principal Officer.

SECTION B: DEFINITIONS

5 For the purpose of this Policy, definition of various terms used shall be as under:

5.1 **'Aadhaar Act'** means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

5.2 **'Aadhaar number'** shall have the meaning assigned to it in clause (a) of Section 2 of the Aadhaar Act and, currently, it means a twelve-digit identification number issued to an individual under sub-section (3) of Section 3 of the Aadhaar Act and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the UIDAI in such manner as may be specified by it.

5.3 **'Authentication'** means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository of the UIDAI for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

5.4 '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 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 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation- For the purpose of this subclause, "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 off 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, and the beneficiaries with 10 percent or more interest in the trust and are other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

5.5 **'Board'** shall mean the Board of Directors of the Company.

5.6 **'Cash Transaction'** for reporting under the PMLA/ PML Rules shall mean the following:

(a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

(b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency.

5.7 **'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 an official of the Company as per the provisions contained in the PMLA.

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:

(i) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,

(ii) branches of overseas banks with whom Indian banks have relationships,

(iii) Notary Public abroad,

(iv) Court Magistrate,

(v) Judge,

(vi) Indian Embassy/ Consulate General in the country where the non-resident customer resides.

5.8 **'Central KYC Records Registry'** ("**CKYCR**") means a reporting entity, substantially owned and controlled by the Central Government, and authorized by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client in such manner and to perform such other functions as may be required under the PML Rules.

5.9 **'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.

5.10 **'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.

5.11 **'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 rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected 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.

5.12 **'Customer Identification'** means undertaking the process of CDD.

5.13 **'Customer Information File'** ("**CIF**") or **'Unique Customer Identification Code'** ("**UCIC**") shall mean a unique code provided by the Company to each of the customers while entering into an account-based relationship with a customer in order to maintain identification records at the customer level.

5.14 **'Designated Director'** means, as defined under rule 2(ba) of the PML Rules. the Managing Director or a whole-time Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the PML Rules.

5.15 **'Digital KYC'** means the capturing live photo of the customer and the OVD 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 official of the Company as per the provisions contained in the PMLA.

5.16 **'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).

5.17 **'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.

5.18 **'FIU-IND'** or '**FIU**' shall mean Financial Intelligence Unit-India.

5.19 **'Know Your Client (KYC) Identifier'** means the unique number or code assigned to a customer by the CKYCR.

5.20 **'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.

5.21 '**Non-Profit Organisations**' means any entity or organisation, constituted for religious or charitable purposes ('*to include relief of the poor, education, medical relief, preservation of environment (including watersheds, forests and wildlife) and preservation of monuments or places or objects of artistic or historic interest, and the advancement of any other object of general public utility*') 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).

5.22 **'Officially Valid Document' ("OVD")** means OVD as defined under rule 2(l)(d) of the PML Rules and the amendments thereto. Currently, OVD means the following:

(a) Proof of possession of Aadhaar number, in such form as issued by the UIDAI;

(b) Passport;

(c) Driving License;

(d) Voter's Identity Card issued by the Election Commission of India;

(e) Job Card issued by NREGA duly signed by an officer of the State Government; and

(f) Letter issued by the National Population Register containing details of name and address.

*"Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address (hereinafter referred to as "**Deemed OVD**"):*

(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 licence agreements with such employers allotting official accommodation.

Provided, the customer shall submit OVD with current address within a period of three months of submitting the alternate documents specified above.

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

5.23 'Offline Verification' means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the UIDAI under the Aadhaar Act.

5.24 'On-going Due Diligence' means regular monitoring of transactions in accounts to ensure that those are consistent with the Company's knowledge about the customers, customers' earning/ business, risk profile and source of funds/ wealth.

5.25 '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 RBI.

5.26 'Person' has the same meaning as defined in the PMLA and includes:

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm

(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within anyone of the above persons {(i) to (v)}, and

(vii) any agency, office or branch owned or controlled by any of the above {(i) to (vi)}.

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

5.28 'PMLA' means the 'Prevention of Money-Laundering Act, 2002', and amendments thereto.

5.29 'PML Rules' or **'Rules'** means the 'Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and amendments thereto.

5.30 'Principal Officer' ("**PO")** means, as defined under rule 2(f) the Rules, an officer at the management level designated by the Board of Directors of the Company for overseeing and managing the KYC and AML Policy and related procedures.

5.31 'Regulated Entities' ("**REs**") mean:

(i) All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs)/ State and Central Co-operative Banks (StCBs/ CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks';

(ii) All India Financial Institutions (AIFIs);

(iii) All NBFCs including Housing Finance Companies, Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs);

(iv) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers);

(v) All authorised persons (APs), including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the RBI.

5.32 'Senior Management' shall mean personnel of the Company who are members of its core management team, excluding Board of Directors, comprising all such persons one level below the Managing Director ("**MD**")/ Executive Directors/ Chief Executive Officer ("**CEO**"), including the departmental heads.

5.33 'Suspicious Transaction' means, as defined under rule 2(g) of the PML Rules, a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(i) Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved; or

(ii) Appears to be made in circumstances of unusual or unjustified complexity; or

(iii) Appears to have no economic rationale or bona fide purpose; or

(iv) 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.

5.34 'Transaction' means, as defined under rule 2(h) of the PML Rules , which means purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

(i) Opening of an account;

(ii) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or cheque or payment order or other instruments or by electronic or other nonphysical means;

(iii) Use of a safety deposit box or any other form of safe deposit;

(iv) Entering into any fiduciary relationship;

(v) Any payment made or received in whole or in part of any contractual or legal obligation;

(vi) Any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and

(vii) Establishing or creating a legal person or legal arrangement.

5.35 'UIDAI' means 'Unique Identification Authority of India'.

5.36 'Video based Customer Identification Process' ("V-CIP') means an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company by undertaking 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 furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of the RBI KYC Directions.

5.37 'Walk-in Customer' means a person who does not have an account-based relationship with the Company but undertakes transactions with the Company.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949 or the Reserve Bank of India Act, 1934 or the PMLA and the PML Rules, any statutory modification or re- enactment thereto or as used in commercial parlance, as the case may be.

SECTION C: GOVERNANCE FRAMEWORK

6 Roles and responsibilities of various authorities of the Company shall be as under:

6.1 The Board of Directors of the Company ("Board") shall be responsible for the following:

(a) To review and approve the Policy as and when required.

(b) To consider and appoint the Designated Director and the Principal Officer.

(c) To delegate any authority for review, approval, and implementation of the Policy.

6.2 The Risk Management Committee ("RMC") shall be responsible for the following:

(a) To review status of compliance with key provisions of the RBI KYC Directions.

(b) To guide the Company for managing money laundering and terrorist financing risks.

6.3 The Senior Management of the Company shall be responsible for the following:

(a) Implementation of the KYC and AML Policy and related procedures.

(b) Decision-making functions with respect to compliance with KYC norms are not outsourced.

6.4 Designated Director- The Designated Director appointed by the Board of Directors shall be responsible for overall compliance with the obligations prescribed by the PMLA and the PML Rules. The Designated Director shall consider, review, and approve various procedures required for the implementation of this Policy.

6.5 Principal Officer- The Company shall designate one of its officials as the Principal Officer of the Company. Key Responsibilities of the Principal Officer ("**PO**") shall be as under:

(a) The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

(b) The PO shall initiate amendments to the Policy based on latest applicable provisions of the PMLA, the PML Rules and RBI KYC Directions, as and when required.

(c) The PO, with the assistance of relevant functions, to ensure implementation of the KYC & AML policy and to consider, review and recommend various procedures which may be necessary for implementation of the Policy.

(d) To ensure submission of periodical reports to the Board/ RMC.

6.6 Employees- The employees of the Company, while delivering their official responsibilities, shall be required to comply with this KYC and AML Policy and other procedures defined by the Company for implementation of the Policy.

6.7 Agents/ Representative of the Company- The Company's agents or persons authorized to represent the Company shall be required to ensure adherence with the KYC & AML Policy. As an when required, such agents/ representatives shall make requisite information available to the RBI/ NHB officials.

SECTION D: CUSTOMER ACCEPTANCE POLICY

7 The Company shall adhere to the following policy guidelines before accepting a customer:

(a) The Company shall not accept a customer who is anonymous or has fictitious or 'benami' name(s).

(b) If the Company is unable to apply appropriate measures for due diligence of the customer either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer, it shall not establish the business relationship.

(c) The Company shall conduct appropriate due diligence of customer and it shall not transact or undertake the account-based relationship without proper diligence as per this Policy.

(d) Due diligence as per this Policy shall also be made applicable to all the co-applicants/ co-borrowers and guarantors, wherever applicable.

(e) Any other additional information, which is not specified in this Policy, shall be obtained with the explicit consent of the customer.

(f) Required details/ information shall be sought by the Company at the time of establishing the business relationship as well as during the periodic updation of KYC.

(g) A CIF/ UCIC shall be allotted while entering into new relationships with customers. However, the Company shall not issue UCIC to occasional customers such as purchasers of third-party products.

(h) The Company shall conduct due diligence at the UCIC level. Thus, if an existing KYC compliant customer desires to open another business relationship with the Company, there shall be no need for a fresh CDD exercise.

(i) The Company shall ensure that necessary checks before opening a new account to ensure that the identity of the customer does not match any person with a known criminal background or with banned entities as per the prescribed lists. Full details of accounts/ customers bearing resemblance with

any of the individuals/ entities in the list shall be reviewed and reported if found suspicious or matching with any entry in the sanction list.

(j) The nature and extent of due diligence to be conducted, at the time of initiation of business relationship, would depend upon risk category of the customer and involve collection/ verification of information by using reliable independent documents, data, or information. Appropriate measures shall be adopted for Enhanced Due Diligence of customers which are deemed high risk from a money laundering perspective.

(k) It shall ensure that it obtains only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the regulatory requirements. The customer profile and information collected shall be treated as confidential and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the customer.

(l) The purpose of commencing of business relationship shall be established and the beneficiary of the relationship/ transaction shall also be identified.

(m) The Company shall conduct due diligence of the third person also who is authorized to act on behalf of a customer as a mandate holder or authority holder.

(n) 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 not further extend/ establish the business relationship. 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.

(o) Where a Permanent Account Number is obtained, the same shall be verified from the verification facility of the issuing authority.

(p) Where Goods and Services Tax ("**GST**") details are available, the GST number shall be verified from the search/ verification facility of the issuing authority.

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

8 Where the Company forms a suspicion of money laundering, and it reasonably believes that performing a due diligence will tip-off the customer, it shall not pursue the due diligence process, and instead report the instance as suspicious transaction with the FIU.

9 The Company shall ensure that its Policy does not result in the denial of financial facility to the people from the financially or socially disadvantaged segments of the society.

SECTION E: RISK MANAGEMENT AND RISK BASED APPROACH

10 Screening of the customers against the Sanctions List

10.1 Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967- In terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, the Company shall screen details of its proposed and existing customers (as and when required) against the details of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are periodically circulated by the United Nations Security Council (UNSC).

The Company shall ensure compliance with the reporting, if any applicable, and other requirements mentioned in latest order of the Govt. of India on Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 *(enclosed with the RBI KYC Directions as its **Annex II**)*.

10.2 Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act, 2005")

(a) The Company shall ensure compliance with the latest order of the Govt. of India on 'Procedure for Implementation of Section 12A' of the WMD Act, 2005, *(enclosed with the RBI KYC Directions as its Annex III)*.

(b) In accordance with paragraph 3 of the aforementioned Govt. 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.

(c) 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 any of individuals and entities in the designated list is customer of the Company.

(d) In case of 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 Director, FIU-India (*designated as the Central Nodal Officer, the authority to exercise powers under Section 12A of the WMD Act, 2005*). A copy of the communication shall be sent to the State Nodal Officer, where the account / transaction is held and to the RBI. Further. the Company shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through, or attempted.

(e) For the above purposes. the Company shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) 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 Director, FIU-India by email and by post, without delay.

(g) In case any order received by the Company from the Director, FIU-India, the Company shall, without delay, take necessary action to comply with the Order.

10.3 The Company shall consider the latest sanction lists prescribed under the RBI KYC Directions including those provided at the following links:

(i) https://scsanctions.un.org/938w9en-all.html

(ii) https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm

(iii) https://www.mha.gov.in/en/page/individual-terrorists-under-uapa

(iv) List of Banned Organisations/Individuals provided at the link: https://www.mha.gov.in/en/divisionofmha/counter-terrorism-and-counter-radicalization-division#

11 Risk Categorization of customers

The Company shall categorise its customers under low, medium or high-risk categories, based on the assessment, profiling and the money laundering risk perceived by it in terms of applicable provisions of the PMLA, PML Rules and the RBI KYC Directions.

For assessing the appropriate risk categories, the Company shall ensure that various information/ details collected from different categories of customers relating to the perceived risk, are non-intrusive. Further, the risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

11.1 High Risk Category

Illustrative Example of high risk customers are as under:

(a) Customers whose KYC details match with the criminals/ terrorists mentioned in the sanction lists prescribed in the RBI KYC Directions (as illustrated under Paragraph 10 above of this Policy).

(b) Non-face to face customers including non-resident customers.

(c) High Net Worth individuals, with annual income/ turnover/ receipts of more than ₹2 crore.

(d) Politically Exposed Persons (PEP).

(e) Those with dubious reputation as per public information available.

(f) Firms with Sleeping partners.

(g) Dealers in high value or precious goods (e.g. jewels, gem and precious metals dealers, art and antique dealer, high value real estate brokers).

(h) Arms manufacturers and dealers.

(i) Trust, Charities, NGO and organization receiving donations.

11.2 Medium Risk Category

Illustrative Example of medium risk customers are as under:

(a) Self-employed non-professionals having no documented income proof (whose income is assessed) and with loan amount above ₹25 Lakh.

(b) Stockbrokers with loan amount above ₹25 Lakh.

(c) Real Estate Agents/ Brokers with loan amount above ₹25 Lakh.

(d) Used Car Dealership with loan amount above ₹25 Lakh.

(e) Custom Brokers with loan amount above ₹15 Lakh.

11.3 Low Risk Category

For the purpose identifying low risk customers will be individual and entities whose identities and source of income can be easily identified. All other customers who do not fall under the high risk and medium risk category shall be categorised as low risk customers. Illustrative examples of low-risk customers are as under:

(a) Borrowers belonging to economically weaker sections and lower income groups with loan amount upto ₹25 Lakh.

(b) Salaries employees whose salary structures are well defined and payment of salary through bank credits/ cheques.

SECTION F- CUSTOMER IDENTIFICATION AND CUSTOMER DUE DILIGENCE

12 Before entering into a business relationship, the Company shall obtain sufficient information necessary to assess the identity and address of a customer as well as the purpose of business relationship. The Company shall apply customer identification procedures in accordance with the RBI KYC Directions.

The Company shall obtain Officially Valid Documents, depending on legal constitution of the respective customer, in accordance with the regulatory requirements. Accordingly, the Company shall conduct Customer Due Diligence to verify the customer's identity, beneficial owner and location along with such other documents pertaining to the nature of business or financial status as may be specified by the Company.

13 Policy Guidelines for Customer Due Diligence ("CDD") if the Customer is an Individual

The policy norms detailed this paragraph shall be applicable to an individual if he/ she is a customer or is a beneficial owner or an authorized signatory/ power of attorney holder on behalf of a legal entity, proposed as the customer.

13.1 For CDD of an individual, the Company shall carry-out the following activities:

(a) Photograph - One recent photograph of the customer shall be obtained.

(b) Permanent Account Number ("PAN")- PAN or the equivalent e-document thereof shall be obtained. If PAN has not been obtained by the customer, then Form No. 60 as defined in Income-tax Rules, 1962 shall be taken.

(c) Officially Valid Documents ("OVD" or "KYC documents") to be obtained- In addition to the above, certified copy of one of the OVDs or the equivalent e-document thereof or one of the following shall be taken for verification of the identity and the address:

(i) The Aadhaar Number where:

(a) If customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act; *or*

(b) If customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company notified under first proviso to sub-section (1) of Section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI; *or*

(ii) Proof of Possession of Aadhaar number where offline verification can be carried out; *or*

(iii) Proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; *or*

(iv) If a customer submits a KYC Identifier, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless:

(a) there is change in the information of the customer vis-à-vis that existing in the records of CKYCR; *or*

(b) the current address of the customer is required to be verified; *or*

(c) the respective credit approving authority of the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer; *or*

(d) validity period of documents downloaded from the CKYCR has lapsed.

(d) Other requirements to be complied with respect to various KYC documents

(i) Aadhaar number may specifically be obtained in the following scenarios:

(a) If customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act; *or*

(b) If a customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company is notified under first proviso to sub-section (1) of Section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI.

(ii) Authentication using e-KYC authentication facility provided by the UIDAI- As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI (under first proviso to sub-section (1) of Section 11A of the PMLA), it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the Aadhaar Act/ RBI KYC Directions. Further, in such a case, if a customer wants to provide a current address, different from the address as per the information available with the UIDAI, he shall provide a self-declaration to that effect to the Company.

(iii) If the customer submits his/ her Aadhaar number, the Company will ensure such customer to redact or blackout his/ her Aadhaar number where the authentication of Aadhaar number is not required under Section 7 of the Aadhaar Act.

(iv) The use of Aadhaar, proof of possession of Aadhaar etc. shall be in accordance with the Aadhaar Act and other applicable regulations/ rules.

(v) If proof of possession of the Aadhaar has been submitted by a customer, the Company shall carry out offline verification wherever possible.

(vi) Where a customer has submitted 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 take a live photo as specified under the Digital KYC Process prescribed below.

(vii) Where a customer submits any OVD or proof of possession of Aadhaar number and its offline verification of such OVD/ proof of possession of Aadhaar cannot be carried out, the Company shall have option to carry-out verification through the Digital KYC Process.

13.2 Digital KYC Process

If the Company implements/ adopts Digital KYC Process, it shall adhere to the following requirements:

(a) The Digital KYC application would be made available at customer touch points for undertaking KYC of its 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 shall ensure that the same is not used by any unauthorized persons. The Application

should be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

(c) The customer, for the purpose of KYC, will be required to visit the location of the authorized official of the Company or vice-versa. The original OVD should be in the possession of the customer.

(d) For this process, it shall be ensured that the Live photograph of the customer is taken by its authorized official and the same photograph is embedded in the Customer Application Form ("**CAF**"). Further, the system application of the Company should put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by the 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 should 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), should be captured vertically from above and water-marking in readable form as mentioned above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

(g) The live photograph of the customer and his original documents should be captured in proper light so that they are clearly readable and identifiable.

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

(i) Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/ her own mobile number, then the 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. It shall be checked that the mobile number used in customer signature should not be the mobile number of the authorized officer.

(j) The authorized officer should provide a declaration about the capturing of the live photograph of the customer and the original document. For this purpose, the authorized official will be required to verify authenticity with a One Time Password (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.

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

(l) The authorized officer of the Company shall check and verify that:

(i) information available in the picture of document is matching with the information entered by authorized officer in CAF;

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

(iii) all of the necessary details in CAF including mandatory field are filled properly.

(m) On successful verification, the CAF shall be digitally signed by an 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.

13.3 Video based Customer Identification Process (V-CIP)

The Company may undertake V- CIP to carry- out CDD in the following situations:

(a) In case of onboarding of new customers such as individual customer, the proprietor in case of a proprietorship firm, authorized signatories, and the BOs if customer is a legal entity.

(b) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication mentioned above.

(c) Updation/ Periodic updation of KYC for customers, as applicable from time to time.

13.3.1 V-CIP Infrastructure

(i) The Company shall comply with the applicable directions prescribed by the RBI on minimum baseline cyber security and resilience framework.

(ii) The technology infrastructure shall be housed in own premises of the Company, unless cloud deployment model is used, and the V-CIP connection and interaction should necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with the applicable RBI directions/ guidelines. If cloud deployment model is used, it shall be ensured that the 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 no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

(iii) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer's consent should be recorded in an auditable and alteration-proof manner.

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

(v) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP should be adequate to allow identification of the customer beyond doubt.

(vi) The application should 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. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

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

(viii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In) and shall be in conformity with the applicable regulatory guidelines.

(ix) The V-CIP application software and relevant APIs/ webservices should also undergo appropriate testing of functional, performance, maintenance strength before being used in a live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal policy and applicable regulatory guidelines.

13.3.2 V-CIP Procedure

(a) The Company shall adhere to these V-CIP procedures and shall have a clear workflow in this regard. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official should be capable of carrying out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

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

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

(d) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

(e) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at an appropriate stage of workflow.

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

(i) OTP based Aadhaar e-KYC authentication.

(ii) Offline Verification of Aadhaar for identification.

(iii) KYC records downloaded from CKYCR, as prescribed, using the KYC identifier.

(iv) Equivalent e-document of OVDs including documents issued through Digilocker.

(g) 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. Accordingly, the Company shall also ensure that the video process of the V-CIP is undertaken within 3 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. The Company shall ensure that no incremental risk is added due to this.

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

(i) Use of printed copy of equivalent e-document including e-PAN shall not be considered valid for the V-CIP.

(j) 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.

(k) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.

13.3.3 V-CIP Records and Data Management

(i) The entire data and recordings of V-CIP shall be stored in a 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.

(ii) For V- CIP also, the Company shall comply with extant regulatory requirements relating to record management.

(iii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

13.4 If the Company opens an account of a customer by using the Aadhaar OTP based e-KYC, in Non-Face-to-Face Mode, it shall comply with the specific directions issued under the RBI KYC Directions for such KYC verification.

14 Policy Norms for CDD of a Sole Proprietary firm as the Customer

14.1 CDD of the proprietor**-** For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) should be carried out as specified in Paragraph 13 of the Policy.

14.2 Proof of business/ activity for the firm- 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) GST/ CST/ VAT certificate.

(e) Certificate/ Registration document issued by Sales Tax/ Service Tax/ Professional Tax authorities.

(f) 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, landline telephone bills etc.

Provided, in cases where the Company is satisfied that it is not possible to furnish two such documents as mentioned above, it may accept only one of those documents as proof of business/ activity, subject to contact point verification and collection of such other information and clarification as would be required to establish the existence of such firm. Further, it should be satisfied that the business activity has been verified from the address of the proprietary concern.

15 Policy Norms for CDD of a Company as the Customer

A company as a customer shall be required to submit certified copies of the following documents/ information:

(a) Certificate of incorporation.

(b) Memorandum and Articles of Association.

(c) PAN of the applicant company.

(d) A resolution from the Board of Directors of the applicant company and power of attorney/ authority granted to its managers, officers or employees to transact on its behalf.

(e) Documents, as specified in Paragraph 13 of the Policy (as applicable to an individual), with respect to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the applicant company's behalf, for a transaction with the Company.

(f) Names of the relevant persons holding senior management position.

(g) Registered office and the principal place of its business, if it is different.

16 Policy Norms for CDD of a Partnership Firm as the Customer

A partnership firm as a customer shall be required to submit certified copies of the following documents:

(a) Registration Certificate, if the deed is registered; or Certificate of Incorporation issued by the Registrar of Companies.

(b) Partnership Deed, or LLP Agreement between the partners or between the LLP and its partners.

(c) Permanent Account Number of the partnership firm.

(d) Documents, as specified in Paragraph 13 of the Policy (as applicable to an individual), with respect to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the firm's behalf, for transaction with the Company.

(e) Partnership Declaration signed by all the partners (all pages should be on the letterhead and should be signed by all the partners).

(f) List of Partners along with capital/profit percentage (to be signed by all partners).

(g) The names of all the partners and address of the registered office.

(h) The principal place of its business, if it is different.

17 Policy Norms for CDD of a Trust as the Customer

A trust as a customer shall be required to submit certified copies of the following documents:

(a) Registration Certificate.

(b) Trust Deed.

(c) Permanent Account Number or Form No.60 of the trust.

(d) Documents, as specified in Paragraph 13 of the Policy (as applicable to an individual), with respect to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the trust's behalf, for a transaction with the Company.

(e) The names of the beneficiaries, trustees, settlor, protector, if any, and authors of the trust.

(f) The address of the registered office of the trust.

(g) The list of trustees and documents, as specified in Paragraph 13 of the Policy, for those discharging the role as trustee and authorised to transact on behalf of the trust.

Further, the Company shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions.

18 **If a customer is an unincorporated association (unregistered trusts/ partnership firms etc.) or a body of individuals (societies etc.),** it shall be required to submit certified copies of the following documents:

(a) Resolution of the managing body of such association or body of individuals.

(b) Power of attorney granted to him to transact on its behalf.

(c) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.

(d) Documents, as specified in Paragraph 13 of the Policy (as applicable to an individual), with respect to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the entity's behalf, for transaction with the Company.

(e) Such information as may be deemed fit by the credit approving authority of the Company to collectively establish the legal existence of such an association or body of individuals.

19 **Policy Norms for opening accounts of a customer who is juridical person (not specifically covered in the earlier part), such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust,** certified copies of the following documents shall be obtained and verified:

(a) Document showing name of the person authorised to act on behalf of the entity;

(b) Documents, as specified in Paragraph 13 of the Policy (as applicable to an individual), with respect to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the entity's behalf, for transaction with the Company; and

(c) Such documents as may be deemed fit by the respective credit approving authority of the Company to establish the legal existence of such an entity/ juridical person.

20 **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 to verify his/ her identity shall be undertaken while considering the following aspects:

(a) Where the customer or the owner of the controlling interest is one of the following:

(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.

(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.

21 Reliance on Customer Due Diligence done by a Third Party

For verifying the identity of customers before establishing an account-based relationship, the Company may also rely on the CDD by a third party, only if the following conditions are met:

(a) 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 PMLA.

(b) 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 CKYCR.

(c) 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.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

22 Validity of KYC Due Diligence done by the Company

KYC verification if done once by one branch/ office of the Company or done for one account shall be valid for its any other branch/ office/ account, provided complete KYC verification has already been done for the concerned account and the same is not due for periodic updation.

SECTION G: ENHANCED DUE DILIGENCE PROCEDURES

23 Enhanced Due Diligence ("EDD") for Higher Risk Customers

The Company, for its medium and high-risk customers, shall conduct risk based Enhanced Due Diligence ("**EDD**") in addition to the CDD. Any business relationship with a high risk or medium risk customers as shall require approval from a credit approving authority who should be at least at the regional or zonal level. Further, any suspicious triggers relating to higher risk customer's transactions shall be reviewed more rigorously.

For higher risk customers, as part of the EDD measures, the Company shall collect additional information and documentation regarding the following if already not collected as part of CDD:

(i) Purpose of the account/ end-use.

(ii) Source of income/ funds.

(iii) Review of income/ financial statements and banking statements.

(iv) Diligence regarding the customer's workplace/ business and business operations.

(v) Proximity of the customer's residence, place of employment, or place of business.

(vi) Due diligence of the individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors, if any.

Further, as part of the EDD procedures, the Company shall follow a system of periodic updation of KYC information for various categories of the customers as prescribed in this Policy.

EDD is an ongoing process, and the Company should take measures to ensure that information is updated as required and that appropriate risk-based monitoring occurs to ensure that any suspicious activity is escalated, analyzed and reported, as prescribed in the Policy.

24 **Requirements relating to the Accounts of Non-Face-to-Face Customers** *(other than Aadhaar OTP based on-boarding as per Paragraph 13.4 of this Policy)*

Non-face-to-face onboarding shall mean establishing 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 includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. The Company shall adhere to the following EDD measures for non-face-to-face customer onboarding (other than Aadhaar OTP based on-boarding done in terms with the Paragraph 13.4 of this Policy):

(a) If the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. Such V-CIP shall be treated on par with face-to-face CIP for the purpose of the RBI KYC Directions.

(b) Transactions shall be permitted only from the mobile number used for account opening. For any change in the mobile used for accounting opening, the following process shall be adopted for due diligence:

(i) The request for change in the mobile number may be considered only after the customer completes the CDD as per Paragraph 13.1 or V-CIP as per Paragraph 13.3 of the Policy; *or*

(ii) The customer may log-in through customer portal or mobile app of the Company and place request for change in the mobile number. Once such a request is placed through the customer portal or mobile app of the Company, the existing mobile number and new mobile number shall be verified through separate OTP.

(c) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

(d) The PAN of the customer shall be verified from the verification facility of the issuing authority.

(e) The Company shall ensure that the first transaction in such accounts shall be a credit from an existing KYC-complied bank account of the customer.

(f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

25 Accounts of Politically Exposed Persons (PEPs)

The Company, before establishing a relationship with PEPs (whether as customer or beneficial owner), shall fulfil the following requirements:

(a) Shall obtain adequate information about prospective customers and sources of funds to determine whether the customer or the beneficial owner is a PEP.

(b) A business relationship with a PEP shall be established only with the approval of an official from the Senior Management.

(c) All such accounts are subjected to enhanced monitoring on an on-going basis.

(d) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, approval shall be obtained from the Chief Credit Officer or National Credit Head to continue the business relationship.

(e) The CDD and EDD measures applicable to a higher risk customer shall be carried out.

The above will also be applicable to accounts where a PEP is the beneficial owner or to the account of a relative/ family members/ close associates of a PEP.

SECTION H: ON-GOING DUE DILIGENCE AND MONITORING OF TRANSACTIONS

26 The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with its knowledge about its customers, their business/ employment and risk profile, and source of funds/ wealth. The Company shall pay special attention to complex, and unusual transactions/ patterns which

have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer.

27 Monitoring of Transactions

The Company shall monitor customers' transactions to identify the following triggers:

(a) Cash repayments above certain thresholds.

(b) Complex transactions with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(c) Loan closure within very short time-period of availing the loan.

(d) Frequent prepayments above some thresholds not consistent with the customer's repayment capacity.

(e) Frequent cash repayments.

28 Monitoring vis-à-vis the Negative List or Adverse Information Received

The Company shall monitor the following instances:

(i) Probable match of a customer's identity with the details provided in the UN Sanctioned Terrorist List or any of the negative lists prescribed by the RBI.

(ii) Any material complaint or alert received against a customer of the Company.

(iii) Query or information received from a Law Enforcement Agency regarding a customer of the Company.

29 Periodical Review of Risk Categorization

The Company will put in place a system of periodical review of risk categorization of accounts. The Company will carry out such a review of risk categorization of customers at a periodicity of not less than once in six months. In case of higher risk perception on a customer, the Company shall assess the need for applying enhanced due diligence measures.

30 Periodic Updation of KYC

The Company shall conduct periodic updation of KYC documents at least once in every 2 years for high-risk customers, once in every 8 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. In this manner, the Company shall follow a risk-based approach for periodic updation of KYC and ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

For updation of KYC documents, the Company, shall ensure compliance with the following:

30.1 Periodic Updation of KYC for Individual Customers

(a) No change in KYC information: If no change in the KYC information, a self-declaration from the customer in this regard shall be obtained. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc.

(b) Change in address: In case of a change in address of the customer, a self-declaration of new address shall be obtained from the customer. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc. Thereafter, the Company shall get the declared address verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. However, due to its inability to conduct contact point verification/ address verification or any reason as per the discretion of any Senior Management official or the Principal Officer, the Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

(c) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. It may be noted that the conditions stipulated in Paragraph 13.4 of this Policy shall be not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. However, 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.

30.2 Periodic Updation of KYC for Non- Individual Customers

(a) No change in KYC information: If no change in the KYC information of the non-individual customer, a declaration/ letter from an official authorized by such customer along with a copy of the board resolution etc., as applicable, shall be taken. The declaration may be taken through letter or through its email-id/ mobile number registered with the Company or through the Company's digital channels, if available, e.g., customer portal/ mobile application of the Company etc.

(b) Beneficial Ownership ("BO") information: The Company shall take steps to keep BO information available with them accurate and updated, as far as possible.

(c) Change in KYC information: In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new non- individual customer.

30.3 In addition to the above, the Company shall take the following measures:

(a) KYC updation shall also be applicable when there is no change in customer information but the documents available with the Company are not as per the current CDD standards.

(b) 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 on-boarding a new customer.

(c) The customer's PAN details, if available with the Company, shall be verified from the database of the issuing authority at the time of periodic updation of KYC also.

(d) In case of receipt of the updated KYC information/ documents, the Company shall provide an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the Company shall ensure that the information/ documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records/ database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

(e) In order to ensure customer convenience, the facility of periodic updation of KYC may be made available at any branch or through any of the online/ digital/ electronic channels of the Company, subject to compliance with the RBI KYC Directions.

(f) The Company, in order to comply with the PML Rules, shall bind its customers, through a loan agreement or any other relevant document, that, in case of any update in the KYC information/ documents submitted by the customer at the time of establishment of business relationship or last submitted, the customers shall be required to submit to the Company the update of such documents, within 30 days of the update to such documents.

SECTION I: REPORTING OF PRESCRIBED TRANSACTIONS/ INFORMATION

31 Details of Designated Director and Principal Officer to be Reported

The Company shall communicate the name, designation, address and contact details of the Designated Director and the Principal Officer to the FIU and the RBI.

32 Reporting of Match with the Prescribed Negative/ Terrorist Lists

Details of customers matching with any of the individuals/entities featuring in the negative/ terrorist lists shall be reported to the National Housing Bank, the FIU-IND

apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 *(as per the Annex II of the RBI KYC Directions)*.

33 Reporting of Prescribed Transactions to the Financial Intelligence Unit-India

In terms with the provisions of the PMLA and the PML Rules, the Company shall furnish the following reports, as and when required, to the FIU-IND:

33.1 Reporting of Cash Transaction above ₹10 Lakh- For the following transactions, the Company shall file the Cash Transaction Report **("CTR")** which for a month should reach to the FIU-IND by 15th day of the succeeding month:

(a) all cash transactions of the value of more than ₹10 Lakh; or

(b) all series of cash transactions integrally connected to each other which have been valued below ₹10 Lakh where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds ₹10 Lakh.

33.2 Reporting of Counterfeit Currency- In addition to the above, all such cash transactions identified 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, if any, shall also be reported by the Company to FIU-IND as Counterfeit Currency Report by 15th day of the succeeding month.

33.3 Reporting of Suspicious Transaction- The Company shall monitor customer transactions to identify suspicious transactions as defined in this policy and the PML rules. the triggers indicating suspicious activity shall be investigated, and, after review/ investigation, a suspicious transaction shall be reported to FIU-IND. The Company shall file the Suspicious Transaction Report **(STR)** to the 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.

34 Confidentiality with respect to the Transactions

The Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records relating to transactions referred to in the preceding paragraph and furnishing of such information to the FIU-IND is confidential. However, such confidentiality requirement shall not inhibit sharing of information to comply with the group-wide programmes against money laundering and terror financing mentioned in paragraph 47 of this Policy. Further, provisions of this paragraph shall also not prevent the Company from sharing the information pertaining to the customers with various agencies/ institutions required in accordance with the other applicable regulatory and statutory provisions/ laws/ regulations/ directions/ rules.

35 Sharing KYC Information with the Central KYC Records Registry (CKYCR)

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

(b) In terms of the provision of Rule 9(1A) of 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.

(c) 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.

(d) The Company shall upload KYC records pertaining to accounts of LEs opened with CKYCR in terms of the provisions of the Rules.

(e) 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.

(f) In order to ensure that all KYC records are incrementally uploaded onto the CKYCR, in case of accounts of individual customers and LEs opened prior to the date when CKYCR upload became effective, the Company shall upload the updated KYC information to CKCYR as and when the same is obtained/ received from such customer at the time of periodic updation.

36 Records pertaining to Non-Profit Organizations, if any, to be reported to DARPAN Portal

If the Company has customers which are non-profit organizations, it shall register details of such customers on the DARPAN Portal of NITI Aayog.

SECTION J: REVIEWS/ RISK ASSESSMENT AND INTERNAL AUDIT

37 Money Laundering ("ML") And Terrorist Financing (TF") Risk Assessment

(a) The Company shall carry out the ML and the TF risk assessment exercise to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, products, services, transactions or delivery channels, etc. The ML and the TF risk assessment shall consider all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The Company, while finalising the internal risk assessment, shall take cognizance of overall sector-specific vulnerabilities, if any, that the regulator/ supervisor may advise from time to time.

(b) The risk assessment shall be commensurate to the nature, size, complexity of activities of the Company and should be properly documented. The risk assessment exercise shall be done at least once in a year.

(c) The outcome of the exercise shall be put up to the RMC. The RMC shall have authority to prescribe controls and procedures in this regard and it shall monitor the implementation of the controls.

(d) Based on its risk assessment, the Company shall put in place policies/ procedures and controls, including CDD, for mitigation and management of identified risks.

38 Internal Audit

The Internal Audit function of the Company shall verify compliance with the KYC and AML Policy. The audit findings and compliance thereof will be put up before the Board or the Audit Committee of the Board on a quarterly interval till closure of audit findings.

SECTION K: RECORD MANAGEMENT

39 Management of the Records relating to Identification of Customers and Transactions

To ensure compliance with the record management requirements prescribed under the PMLA and the PML Rules, the Company shall take the following steps:

(a) The Company shall maintain all necessary records of transactions between the Company and the customer for at least five years from the date of transaction.

(b) The Company shall 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 is ended.

(c) The Company shall maintain proper records of the following types of transactions (which are prescribed under Rule 3 of the PML Rules):

(i) all cash transactions, carried-out at single instance, of the value of more than ₹10 Lakh.

(ii) all series of cash transactions integrally connected to each other which have been valued below Rs.10 lakh where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds ₹10 Lakh.

(iii) all transactions involving receipts by non-profit organizations of ₹10 Lakh.

(iv) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions; and

(v) all suspicious transactions whether or not made in cash or otherwise.

(d) Records to contain the specified information- For the transactions referred in the preceding sub-paragraph, the Company shall maintain all necessary

information so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transaction;

(ii) the amount of the transaction;

(iii) the date on which the transaction was conducted; *and*

(iv) the parties to the transaction.

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

(f) The Company shall maintain the records referred in this paragraph in hard or soft format.

(g) The Company shall make available swiftly, the identification records and transaction data to the competent authorities upon request.

(h) 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.

40 Records pertaining to Non-Profit Organizations to be Maintained

If the Company has customers which are non-profit organizations, the Company shall also maintain such registration records for a period of 5 years after the business relationship between such customer and the Company has ended or closed, whichever is later.

SECTION L: OTHER POLICY GUIDELINES

41 Introduction of New Technologies

The Company, for customer due diligence and on-going due diligence, shall explore to adopt appropriate new technologies including artificial intelligence and machine learning which shall be commensurate to the money laundering risk perceived for the business undertaken by the Company with its customers.

The Company shall identify and assess the ML/ TF risks that may arise with respect to new products, new business practices and the use of new or developing technologies for both new and pre-existing products. In this regard, the Company shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; *and*

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

42 Selling Third Party Products

In case the Company acts as an agent for selling any third-party products (permitted as per the extant regulations), it shall ensure compliance with the following aspects:

(a) The identity and address of the walk-in customer shall be verified as per the extant applicable regulatory requirements before undertaking any transaction.

(b) Transaction details of sale of third-party products and related records shall be maintained.

(c) Monitoring of transactions for any suspicious activity will be done.

43 Quoting of PAN

For cash collection of ₹50,000/- and more from a customer in a single day, to adhere to the Income Tax Rule 114B, the Company shall ensure the following:

(a) If the customer's PAN is not updated in system, PAN of the customer along with a copy of the PAN Card shall be required to be collected for cash receipt of ₹50,000/- or more. Further, the PAN shall be updated in the Company's system.

(b) If the customer is not having PAN, then Form 60 duly signed by the customer along with a valid identity proof shall be collected for cash receipt of ₹50,000/- and more.

44 Hiring of Employees and Employee Training

(a) As an integral part of its personnel recruitment/ hiring process, the Company shall put in place an adequate screening mechanism.

(b) The Company shall make efforts to ensure that the staff dealing with/ being deployed for KYC/ AML/ CFT matters have the following:

(i) high integrity and ethical standards;

(ii) good understanding of extant KYC/ AML/ CFT standards;

(iii) effective communication skills; *and*

(iv) ability to keep up with the changing KYC/ AML/ CFT landscape, nationally and internationally.

(c) The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(d) The Company shall organise employee training programmes so that the members of staff are adequately trained in the KYC and AML Policy requirements. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education.

(e) The Company shall ensure 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.

45 Secrecy Obligations and Sharing of Information

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

(b) 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.

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

(d) 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) The interest of the Company requires disclosure; and

(iv) Where the disclosure is made with the express or implied consent of the customer.

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

The Company shall adhere to the provisions of the Income Tax Rules 114F, 114G and 114H, as and when applicable as a reporting financial institution.

47 Actions to be taken at the Group Level[1]

For discharging obligations under the provisions of Chapter IV of the PML Act, 2002, the Company shall co-ordinate with other group entities and take actions to implement group-wide programmes, within its group, against money laundering and terror financing, including policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk

[1] *"**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), which currently is defined as under:*

"Group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes,- (i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or (ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

management. Further, such programmes shall ensure adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

48 Endeavor to adopt standards and guidance notes issued by the FATF[2]

The Company, while ensuring compliance of the legal/regulatory requirements as above, shall also endeavor to adopt the relevant/ applicable best practices taking into account the standards and guidance notes issued by the Financial Action Task Force ("**FATF**"), for managing risks better.

---XXX---

[2] ***FATF*** *is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.*