CENTRUM HOUSING FINANCE LIMITED

KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML) POLICY

Document Title	**KYC and AML Policy**
Approved/ Reviewed by	**Board of Directors**
Date of Approval/ Review	**28.10.2021**
Version No.	**1.0/ 2021**

1. BACKGROUND AND SCOPE

The 'Prevention of Money Laundering Act, 2002' ("**PMLA**") has enacted and notified by the Government of India 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, various rules called as called the 'Prevention of Money-Laundering (Maintenance of Records Rules), 2005' ("**PML Rules**") have been made 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.

Centrum Housing Finance Limited ("**Company**" or "**CHFL**"), as a Housing Finance (classified as a 'Reporting Entity' under the PMLA) is required to take steps to implement various applicable provisions of the PMLA and the PML Rules.

In this regard, the Reserve Bank of India ("**RBI**") has prescribed the Reserve Bank of India {Know Your Customer (KYC)} Directions, 2016 ("**RBI KYC Directions**") in order to ensure compliance by every entity regulated by RBI ("**REs**") with the provisions of the PMLA and the PML Rules. The RBI KYC Directions has prescribed guidance on various operational aspects relating to the same and has also advised that an RE should adopt 'Know Your Customer' ("**KYC**") Policy duly approved by its Board of Directors or any committee of the Board to which power has been delegated.

In accordance with the latest RBI KYC Directions, CHFL has reviewed its existing 'Know Your Customer ("**KYC**") and Anti-Money Laundering ("**AML**") Policy ("**KYC & AML Policy**") which will supersede all prior versions of the KYC & AML Policy adopted by the Company.

This KYC & AML Policy shall be defining minimum requirements for the Company to establish, implement, and maintain framework and procedures those are appropriately designed to ensure compliance with the applicable laws, rules and regulations relating to KYC & AML standards.

This **KYC & AML Policy** endeavors to cover 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. OBJECTIVES

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

2.2 To know/understand the Customers and their financial dealings better, which in turn, help in managing their risks prudently.

3. APPLICABILITY

This KYC & AML Policy ("**Policy**") shall apply to the Company, its officials, representatives, and any third parties relied upon or used by it to perform any of the requirements prescribed under the RBI KYC Directions. Once approved by the Board of the Company, this version of the KYC & AML Policy shall supersede all earlier versions of the KYC & AML Policy adopted by the Company.

4. DEFINITIONS

For this Policy, definition of various terms used is as under:

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

4.2 **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.

4.3 **"Authentication",** in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar Act.

4.4 **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 25 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 of/ 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 including societies**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/ have ownership of/ entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: 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 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

4.5 **Board** means Board of Directors of the Company.

4.6 **Cash Transaction** 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.

4.7 **Certified Copy**- Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised 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, alternatively, the original certified copy, certified by any one of the following, may be obtained:

(a) Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,

(b) Branches of overseas banks with whom Indian banks have relationships,

(c) Notary Public abroad,

(d) Court Magistrate,

(e) Judge,

(f) Indian Embassy/Consulate General in the country where the NRI/ PIO resides.

4.8 **Central KYC Records Registry (CKYCR)** means an entity defined under Rule 2(1)(aa) of the PML Rules to receive, store, safeguard and retrieve the KYC records in digital form.

4.9 **Counterfeit Currency Transaction-** 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.

4.10 **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.

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

4.12 **Customer identification** means undertaking the process of CDD.

4.13 **Designated Director** means 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.

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.

4.14 **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.

4.15 **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).

4.16 **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.

4.17 **FIU-IND** shall mean **Financial Intelligence Unit-India.**

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

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

4.20 **Non-face-to-face customers-** Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials.

4.21 **Officially valid document (OVD)-** Any document notified/ advised by the Central Government/ Regulatory Authorities as officially valid document for verifying identity and proof of address of customers.

Currently, OVD means the following:

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

ii) Passport;

iii) Driving License;

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

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

vi) 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:

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

b) Property or Municipal tax receipt;

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

d) Letter of 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.*

4.22 **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.

4.23 On-going Due Diligence- Regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

4.24 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.

4.25 Person has the same meaning assigned in the Act and includes:

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

4.26 Politically Exposed Persons- Individuals who are or have been entrusted with prominent public functions, e.g., Heads of States/ Governments, senior politicians, senior government officer (Joint Secretary and above grade)/ judicial (High Court Judge and above)/ military officers (Brigadier/ equivalent rank & above), senior executives of state-owned corporations (Executive Director & above), important political party officials (state level and above) etc.

4.27 PMLA- shall mean the 'Prevention of Money-Laundering Act, 2002', & amendments thereto.

4.28 PML Rules- shall mean the 'Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, & amendments thereto.

4.29 Principal Officer (PO)- An official designated by the Board of Directors of the Company for overseeing and managing the KYC & AML policies and processes. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

4.30 Regulated Entities or **REs** mean:

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

b) All India Financial Institutions (AIFIs);

c) All Non-Banking Finance Companies including Housing Finance Companies ("HFCs"), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs);

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

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

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

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

b) appears to be made in circumstances of unusual or unjustified complexity; or

c) appears to have no economic rationale or bona fide purpose; or

d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds 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.

4.32 Transaction- means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a) opening of an account;

b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

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 of any contractual or other legal obligation;

f) establishing or creating a legal person or legal arrangement.

4.33 UIDAI shall mean 'Unique Identification Authority of India'.

4.34 Video based Customer Identification Process (V-CIP)- 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.

4.35 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 or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re- enactment thereto or as used in commercial parlance, as the case may be.

5. POLICY GOVERNANCE

5.1 Approval Authority and Review of the Policy- The Policy will be approved by the Board initially. Thereafter, it will be reviewed by the Board at least once in a year if not earlier required by the regulatory authorities. 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 is 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.

5.2 Designated Director- The Company shall nominate the Designated Director to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder. Mr. Sanjay Shukla, Managing Director, has, currently, been appointed as the Designated Director of the Company.

5.3 Principal Officer- The Company designate one of its senior officials as the 'Principal Officer' who will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

The name, designation and address of the Designated Director and also the Principal Officer shall be communicated to the RBI/ NHB/ FIU-IND, as and when required.

5.4 Senior Management and Key Responsibilities of the Senior Management

Apart from the Designated Director and Principal Officer, the following officials of the Company have been considered as the 'Senior Management' for the purpose of KYC compliance:

(a) Chief Credit Officer- responsible for overviewing the KYC compliance and suggesting any changes.
(b) National Credit Manager- responsible for obtaining and maintaining all KYC records from the borrowers.
(c) Head- Operations- responsible for obtaining and maintaining all KYC records from the borrowers.
(d) Compliance Officer- responsible for ensuring that the KYC compliance is being met as per regulations prescribed.

It shall also be ensured by the Senior Management that decision-making functions of determining compliance with KYC norms are not outsourced.

6. CUSTOMER ACCEPTANCE POLICY ("CAP") AND CUSTOMER DUE DILIGENCE ("CDD")

The Company shall adhere to the following Customer Acceptance Policy ("**CAP**") criteria for acceptance of customers:

a) The Company shall not open any account(s) in anonymous, fictitious or 'benami' name(s). 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 and endeavour to identify the beneficiary of the relationship/ account.

In this regard, nature and extent of basic due diligence measures to be conducted at the time of opening of account/ business relationship, will depend on the risk category of the customers and shall involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the risks which may be posed by the prospective customer and his/ her expected use of the Company's products and services.

b) No account shall be opened where the Company is unable to apply appropriate Customer Due Diligence ("**CDD**") measures, either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.

c) No transaction or account-based relationship will be undertaken without following the CDD procedure.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation will be specified.

e) Optional or additional information will be obtained with an explicit consent of the customer after the account is opened.

f) CDD Procedure will be followed for all co-applicants, wherever co-applicant is there.

g) If an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, will be clearly spelt out.

i) Suitable system will be put in place to ensure that identity of the customer doesn't 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 will maintain lists of individuals or entities issued as advised by the RBI, from time to time. Details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be reported as may be required.

j) The Company may rely on third party verification subject to the conditions prescribed by the RBI, the PMLA and the Rules thereunder in this regard.

k) For non-face-to-face customers, appropriate due diligence measures will be defined for identification and verification of such customers.

l) The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer. The Company shall maintain confidentiality of information as provided in Section 45NB of the Reserve Bank of India Act, 1934.

m) Appropriate Enhanced Due Diligence ("**EDD**") measures shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear, who are Politically Exposed Persons ("**PEPs**") and their family members/close relatives etc.

n) In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall be adopted.

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

p) 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 (21 of 2000).

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

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

7. RISK MANAGEMENT

7.1 Risk Categories

The Company will categorize its customers as low, medium and high-risk category, in accordance with the applicable regulatory requirements and based on the assessment, profiling and the risk perceived by it. The risk categorization of various profiles will be broadly as under:

7.1.1 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. Illustrative Example of low risk customers are below:

(a) Employees whose salary structures are well defined and payment of salary through bank credits/ cheques.

(b) People belonging to lower economic strata of society whose accounts show small balances and low turnover however with documented income (self-employed non-professionals).

(c) Employed with Government departments and Government owned companies.

(d) Employed with PSU and reputed public limited companies.

(e) Self-employed professionals.

7.1.2 Medium Risk Category

Illustrative Example of medium risk customers are as under:

(a) Salaried employees whose salaries are variable in natures/ contractual /whose income has to be assessed.

(b) Salaried employees who are working with small private limited or LLP or organization of non- repute in nature.

(c) Self-employed non-professionals with sound business and profile.

(d) Self-employed non-professionals having no documented income proof (whose income is assessed).

(e) Employees of Trusts, Charities and NGOs who are with repute.

(f) Companies having close family shareholding.

7.1.3 High Risk Category

Illustrative Example of high risk customers are as under:

(a) Politically Exposed Persons (PEP).

(b) Non-face to face customers.

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

(d) Firms with Sleeping partners.

(e) Trust, Charities, NGO and organization receiving donations

The parameters such as customer's identity, social/ financial status, nature of business activity, and information about the clients' business and their location etc. may be considered in this regard. However, the Company shall ensure that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

7.2 Periodic Review of Risk Categorisation

The Company will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in accordance with the regulatory requirements.

7.3 Review of status of compliance with the KYC & AML Policy

To provide reasonable assurance to the management of the Company that its KYC & AML procedures are functioning effectively, review of the same will be included under the scope of its Internal Audit. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

8. CUSTOMER IDENTIFICATION PROCEDURES ("CIP")

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company will obtain sufficient information necessary to establish the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

The Company will ensure compliance with the regulatory/ statutory requirements with respect to 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. However, the Company shall ensure that introduction is not to be sought while opening accounts.

8.1 The Company shall undertake identification of customers in the following cases:

a) Commencement of an account-based relationship with a customer.

b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

c) Selling third party products as agents, selling their own products, and any other product for more than ₹50,000/- (Rupees Fifty Thousand).

d) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds ₹50,000/- (Rupees Fifty Thousand), whether conducted as a single transaction or several transactions that appear to be connected.

e) When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of ₹50,000/- (Rupees Fifty Thousand).

8.2 Reliance on customer due diligence done by third party

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

a) 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 CKYCR.

b) Copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

c) The third party should be 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.

d) The third party should 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.

9. CUSTOMER DUE DILIGENCE (CDD) PROCEDURES

The Company, depending on legal constitution of the respective customer, will obtain valid KYC documents/ credentials in accordance with the regulatory requirements 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 additionally required by the Company. In case of existing customers if any additional documents are made mandatory by the Govt. of India, the Company shall ensure to obtain the same from the customer. If the same is not provided by the customer due to whatsoever reason, the Company shall take the steps as prescribed by the Govt. of India/ RBI in this regard.

9.1 CDD Procedure in case of Individual *(who is a customer or is a beneficial owner/ authorised signatory/ the power of attorney holder related to any legal entity)*- If the customer is an individual, along with a recent photograph and certified copy of Permanent Account Number (PAN) or the equivalent e-document thereof, certified copy of one of the OVDs or the equivalent e-document thereof as defined above shall be taken for verification of the identity and the address.

9.1.1 Exception for PAN- If PAN has not been availed by the customer, then Form No. 60 as defined in Income-tax Rules, 1962 may be taken.

9.1.2 Aadhaar related provisions

(a) Aadhaar number may be obtained in case of the following:

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

(ii) 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.

(b) The Company, being a non-bank, may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purpose. However, where its customer submits his Aadhaar number, the Company will ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar Act.

(c) 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, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the PMLA/ the Aadhaar Act/ the RBI KYC Directions. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in Central Identities Data Repository of the UIDAI, he may give a self-declaration to that effect to the Company.

Accounts opened using OTP based e-KYC authentication, in non-face-to-face mode, shall be subject to the following conditions:

(i) There must be a specific consent from customer for authentication through OTP.

(ii) Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed Rs.60,000/- in a year.

(iii) Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

(iv) If the CDD procedure as mentioned above is not completed within a year, no further debits shall be allowed.

(v) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, the Company shall clearly indicate that such accounts are opened using OTP based e-KYC.

(vi) The Company shall not open accounts based on the KYC information available in the CKYCR of accounts opened with OTP based e-KYC procedure in non-face-to-face mode, as per the information available.

(d) The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar Act and the regulations made thereunder.

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

9.1.3 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 any rules issues thereunder and take a live photo as specified under the **Digital KYC Process** as detailed subsequently in this Policy**.**

9.2 Digital KYC Process

a) To implement Digital KYC Process, the Company will develop an application which should be made available at customer touch points for undertaking KYC of their customers and the KYC process should be undertaken only through this authenticated application of the Company.

b) The access of the Application should be controlled by the Company, and it should be ensured 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 possession of the customer.

d) For this process, it should 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 should 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 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 customer and the original document. For this purpose, the authorized official will have to be verified with 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 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.

9.3 Video based Customer Identification Process (V-CIP)

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

(i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

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

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

9.3.1 V-CIP Infrastructure

a) To conduct, V-CIP, the Company will ensure compliance with the applicable RBI guidelines on minimum baseline cyber security and resilience framework.

b) The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction should necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall complied with relevant RBI guidelines.

c) 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.

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

e) 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.

f) 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.

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

h) The V-CIP infrastructure should 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 suitably accredited agencies as may be prescribed by RBI and in conformity with internal policy and applicable regulatory guidelines.

i) The V-CIP application software and relevant APIs/ webservices should also undergo appropriate testing of functional, performance, maintenance strength before being used in 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.

9.3.2 V-CIP Procedure

a) The Company shall adhere to these V-CIP procedure 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 to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

b) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session should be 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 appropriate stage of workflow.

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

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 line with the prescribed period of 3 days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within 3 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.

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

9.3.3 V-CIP Records and Data Management

a) 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.

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

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

9.4 CDD Measures for Sole Proprietary firms

9.4.1 For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out as prescribed for an individual customer, detailed above.

9.4.2 Further, any two of the following documents or equivalent e- documents thereof shall also be obtained as a proof of business/ activity in the name of such firm:

i) Registration certificate;

ii) Certificate/ License issued by the municipal authorities under Shop and Establishment Act;

iii) Sales and income tax returns;

iv) CST/VAT certificate;

v) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities;

vi) License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;

vii) 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;

viii) Utility bills such as electricity, water, landline telephone bills etc.

9.4.3 In cases where the Company is satisfied that it is not possible to furnish two such documents from the above list, it may accept only one of those documents as proof of business/ activity, provided 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.

9.5 CDD Measures for other Legal Entities

9.5.1 Where the client is a company, it shall submit certified copies of the following documents or equivalent e- documents thereof:

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; and

e) Documents (same as applicable to an individual customer) for the beneficial owner(s)/ manager(s)/ 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.

9.5.2 Where the client is a partnership firm, it shall submit certified copies of the following documents or equivalent e- documents thereof:

a) Registration Certificate;

b) Partnership Deed;

c) Permanent Account Number of the partnership firm; and

d) Documents (same as applicable to an individual customer) for the beneficial owner(s)/ manager(s)/ officers or employees, as the case may be, holding an attorney to transact on the firm's behalf, for transaction with the Company.

9.5.3 Where the client is a trust, it shall submit certified copies of the following documents or equivalent e- documents thereof:

a) Registration Certificate;

b) Trust Deed;

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

d) Documents (same as applicable to an individual customer) for the beneficial owner(s)/ manager(s)/ officers or employees, as the case may be, holding an attorney to transact on the trust's behalf, for a transaction with the Company.

9.5.4 Where the client is an unincorporated association (unregistered trusts/ partnership firms etc.) or a body of individuals (societies etc.), it shall submit certified copies of the following documents or equivalent e- documents thereof:

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 (same as applicable to an individual customer) for the beneficial owner(s)/ manager(s)/ officers or employees, as the case may be, holding an attorney to transact on the entity's behalf, for transaction with the Company; and

e) Such information as may be required by the reporting entity to collectively establish the legal existence of such an association or body of individuals:

9.5.5 For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or equivalent e-documents thereof shall be obtained:

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

b) Documents (same as applicable to an individual customer) for the beneficial owner(s)/ manager(s)/ 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 required by the R to establish the legal existence of such an entity/ juridical person.

9.6 Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) (as defined under the 'Definitions' provided in the Policy) shall be identified and all reasonable steps to verify his/her identity shall be undertaken keeping in view the following:

9.6.1 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.

9.6.2 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.

9.7 Simplified Procedure for Opening Accounts

In case a person who desires to open an account is not able to produce any of the OVDs, the Company may at its discretion open accounts subject to the following conditions:

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

b) The authorized officer of the Company should certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

c) The account shall remain operational initially for a period of 12 months, within which CDD as prescribed above should be carried out.

d) Balances in all their accounts taken together shall not exceed Rs.50,000/- at any point of time.

e) The total credits in all the accounts taken together shall not exceed Rs.1,00,000/- in a year.

f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

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

10. ENHANCED DUE DILIGENCE (EDD) PROCEDURES

10.1 Accounts of Non-Face-To-Face Customers: In case of a non-face to face customer, for enhanced due diligence, the Company shall ensure that first payment to be affected through the customer's KYC-complied account with another regulated entity.

10.2 Accounts of Politically Exposed Persons (PEPs): The Company will 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 shall have been verified before accepting the PEP as a customer;

c) the decision to open an account for a PEP is taken at the level of Chief Credit Officer or National Credit Head in accordance with the Company's Customer Acceptance Policy;

d) all such accounts are subjected to enhanced monitoring on an on-going basis;

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

f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis shall be applicable.

The above will also be applicable to accounts where a PEP is the beneficial owner.

11. ON-GOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC/ AML policy. 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 & risk profile, and the source of funds.

11.1 On-going Due Diligence and Monitoring of Transactions- The Company, its on-going due diligence, shall consider the following aspects:

(a) The Company will pay 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 shall be aligned with the risk category of the customer. A system of periodic review of risk categorisation of accounts as prescribed in this Policy shall be put in place.

(c) The Company will 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.

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

11.3 Periodic Updation- The Company will conduct periodic updation of KYC documents 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 from the date of opening of the account / last KYC updation.

The Company, in this regard, shall comply with the following standards:

11.3.1 Individual Customers

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

b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id/ mobile number registered with the Company, digital channels such as customer portal/ mobile application of the Company, letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. If the Company, due to any reason is not able to conduct contact point verification/ address verification, then 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.

11.3.2 Non- Individual Customers

a) No change in KYC information: In case of no change in the KYC information of the non- individual customer, a self-declaration in this regard shall be obtained from such customer through its email id registered with the Company or digital channels such as customer portal/ mobile application of the Company, letter from an official authorized by such customer in this regard, board resolution etc.

b) Beneficial Ownership (BO) information - The Company shall take steps to keep Beneficial Ownership (BO) information available with them as accurate and as updated 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.

11.3.3 Additional measures- Further, the Company shall ensure the following:

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

b) Customer's PAN details, if available, will be verified from the database of the issuing authority at the time of periodic updation of KYC.

c) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the information/ documents obtained from the customers at the time of periodic updation of KYC should be promptly updated in the records/ database of the Company and an intimation, mentioning the date of updation of KYC details, should be provided to the customer.

d) 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, as may be permitted under the RBI KYC Directions.

e) The Company shall ensure that its policy guidelines on updation/ periodic updation of KYC are transparent and adverse actions against the customers shall be avoided, unless warranted by specific regulatory requirements.

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

Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, appropriate relaxation(s) will be given with the prior approval of CCO/ CRO for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

12. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

12.1 The Company will capture the KYC information/ details as 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.

12.2 In terms of 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.

12.3 The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be.

12.4 The Company shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules.

12.5 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.

12.6 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.

12.7 Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless:

- **a)** there is a change in the information of the customer as existing in the records of CKYCR;
- **b)** the current address of the customer is required to be verified;
- **c)** the 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 client.

13. MONEY LAUNDERING ("ML") AND TERRORIST FINANCING (TF") RISK ASSESSMENT

13.1 The Company shall carry out the ML) and the TF risk assessment exercise periodically 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 assessment process should 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 also take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

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

13.3 The outcome of the exercise shall be put up to the Risk Management Committee of the Company ("**RMC**").

13.4 The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk. The RMC shall have authority to prescribe controls and procedures in this regard and it shall monitor the implementation of the controls.

14. REPORTING THE FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-IND)

In accordance with the requirements under the PMLA, the Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

14.1 Cash Transaction Report (CTR)- If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

14.2 Counterfeit Currency Report (CCR)- All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

14.3 Suspicious Transactions Reporting (STR)- The Company will monitor transactions to identify potentially suspicious activity. Such triggers will be investigated, and any suspicious activity will be reported to FIU-IND. The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. 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.

The Company will maintain confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the 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 govt. authorities etc.

15. RECORD MANAGEMENT

The Company shall ensure compliance with the following requirements with respect to the Record Management:

(a) The Company shall maintain all necessary records of transactions between it and the customer for at least 5 years from the date of transaction;

(b) It 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 5 years after the business relationship is ended;

(c) It shall make available the identification records and transaction data to the competent authorities upon request;

(d) It shall have a system of maintaining proper record of transactions prescribed under Rule 3 of the PML Rules. Currently, the Rule 3 includes: (i) Cash Transaction; (ii) Suspicious Transaction; and (iii) Counterfeit Currency Transaction, as defined in this Policy;

(e) It shall maintain all necessary information in respect of transactions prescribed under Rule 3 of the PML Rules so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

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

(iv) the parties to the transaction.

(f) It shall evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities; and

(g) It shall maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

16. SCREENING AGAINT THE SANCTIONS LIST

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

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/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

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/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

Details of accounts resembling any of the individuals/ entities in the lists shall be reported to FIU-IND in addition to the Ministry of Home Affairs as required under UAPA notification as provided in the RBI KYC Directions.

17. SELLING THIRD PARTY PRODUCTS

The Company, if acting as agents while selling third party products as per regulations in force from time to time, will comply with the following aspects:

a) The identity and address of the walk-in customer shall be verified for the transactions as required under the CIP prescribed above.

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.

18. QUOTING OF PAN

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

19. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

19.1 Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

19.2 On-going employee training programme shall be put in place so that the members of staff are adequately trained in the KYC and AML Policy. 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. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the Company, regulation and related issues shall be ensured.

20. INTRODUCTION OF NEW TECHNOLOGIES

The Company will pay adequate attention to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favour anonymity, and it shall take measures to prevent its use in money laundering schemes, as may be applicable.

21. ADHERENCE TO KNOW YOUR CUSTOMER (KYC) GUIDELINES BY THE COMPANY'S AGENTS

21.1 The Company's agents or persons authorized by it, for its business, shall be required to be compliant with the KYC & AML Policy.

21.2 All information shall be made available to the RBI/ NHB to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by the Company including agents etc. who are operating on its behalf.

21.3 The books of accounts of persons authorized by the Company including agents etc., so far as they relate to business of the company, shall be made available for audit and inspection whenever required.

22. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

The Company, as and when applicable, will ensure adherence to the provisions of Income Tax Rules 114F, 114G and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take requisite steps for complying with the reporting requirements in this regard.

--- XXX ---