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

(Version 1.9)

CONTENTS

1. INTRODUCTION

TVS Credit Services Ltd (TVSCS, hereinafter referred to as Company or Regulated Entity - RE) has ensured that a proper policy framework on KYC and AML measures is formulated in line with the RBI directions and has been duly approved by the Risk Management Committee. This policy was first adopted by the Board of Directors of the company in the meeting held on 21st April 2010. The policy is subjected to amendment in line with the RBI directions issued from time to time. The policy shall be subject to be reviewed on an annual basis or as and when required.

2. OBJECTIVES

The KYC policy of the Company has been framed taking into account the following objectives;

a. To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.

b. To prevent the Company from being used, intentionally or unintentionally, by criminal elements for Money Laundering (ML) or Terrorist Financing (TF) activities.

c. To enable the Company to know/understand its customers and their financial dealings better, this in turn is expected to help manage the associated risks prudently.

d. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

3. APPLICABILITY

This KYC policy is applicable to all business operations of TVSCS.

4. DEFINITIONS

1) **"Digital KYC"** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the company as per the provisions contained in the Act. The operational guidelines have been given in Annex 1.

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

2) **"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).

3) "**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) **"Officially Valid Document"** (OVD) means;
   i. Passport
   ii. Driving license
   iii. Proof of possession of Aadhaar number.
   Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
   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
   vi. Letter issued by the National Population Register containing details of name and address.

5) **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

6) **"Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

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 officer of the Company as per the provisions contained in the Act.

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

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

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

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

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

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

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors of the company,

b. the Managing Partner, if the Regulated Entity (RE) is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

13) **"Principal Officer"** means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

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

c. appears to not have economic rationale or bona-fide purpose; or

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

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

15) **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of an account;

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

c. the use of a safety deposit box or any other form of safe deposit;

d. entering into any fiduciary relationship;

e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

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

16) **"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 as per RBI directions.

17) **"Common Reporting Standards" (CRS)** means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

18) **"Customer"** means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

19) **"Walk-in Customer"** means a person who does not have an account-based relationship with the company but undertakes transactions with the company.

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

21) **"Customer identification"** means undertaking the process of CDD.

22) **"Group"** The definition of the term "group" has been provided under the amendment having its meaning assigned under Section 286 of the Income Tax Act 1961 (IT Act). As per IT Act, "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. Further, as per Rule 3A of the PMLR Amendment, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money Laundering Act 2002 (PMLA) which deals with obligations of banking companies, financial institutions and intermediaries.

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

24) **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the company or meeting the officials of company.

25) **"Non-profit organization"** means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)."

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

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

Note: Other terms not specifically defined herein shall have the meaning as assigned to them under the RBI KYC Master Directions and the Prevention of Money Laundering Act/Rules.

In addition to the documents stated in this policy, any other documents and information obtained from the customer as part of the company's credit policy will be considered an extension of the KYC policy for the purposes of the information requirements as a part of KYC policy.

5. DESIGNATED DIRECTOR

The Board of the Company has appointed the Chief Executive Officer, as the Designated Director, to ensure overall compliance with the obligations under Prevention of Money laundering Act and Rules framed thereunder, from time to time. The name, designation and address of the Designated Director have been communicated to the FIU-IND and shall also be communicated to the RBI. In no case, the Principal Officer shall be nominated as the 'Designated Director'.

6. PRINCIPAL OFFICER

The Company has appointed the Chief Compliance Officer as the Principal Officer. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, sharing, and reporting information as required under the Prevention of Money Laundering Act and Rules. The name, designation and address of the Principal Officer has been communicated to the FIU-IND and shall also be communicated to the RBI.

All suspicious transactions shall be reported immediately to the Principal Officer of the company for reporting to FIU- IND.

7. COMPLIANCE OF KYC POLICY

The company has constituted Senior Management for the purpose of the KYC compliance in line with the KYC policy. The Internal Audit team shall on a continuous basis conduct an independent evaluation of adherence to KYC compliance requirements and submit quarterly audit notes on compliance to Audit committee. A Concurrent audit system shall be put in place to verify the compliance with KYC/AML policies and procedures.

The Company ensures that decision-making functions of determining compliance with KYC norms at the time of customer identification/customer onboarding are not outsourced.

8. KEY ELEMENTS OF THE POLICY

The policy includes the following key elements:

i. Customer Acceptance Policy (CAP)
ii. Customer Identification Procedures (CIP)
iii. Monitoring of Transactions
iv. Risk Management

8.1. CUSTOMER ACCEPTANCE POLICY (CAP)

The Company's CAP lays down criteria for acceptance of customers. When taking decision to grant any loan facilities to the customers as well as during the continuation of any loan facilities the following norms and procedures shall be followed by the company.

a. No account is opened in anonymous or fictitious/benami name.
b. No account is opened where the Company is unable to apply appropriate Customer Due Diligence measures (CDD), 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 is undertaken without following the CDD procedure as set out in **Para 8.2** of this policy.
d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is obtained as explained in **Paras 8.2 and 13** respectively of this policy.
e. Additional information where such information requirement has not been specified in the KYC Policy and the Credit Policy, shall be obtained with the explicit consent of the customer after the account is opened.
f. A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers and also to the existing customers by the Company. System based de-dupe checks based on customer details available in system shall be put in place. The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.
g. CDD Procedure is followed for borrowers, co borrowers and beneficial owners.
h. The identity of the customer does not match with any person or entity, whose name appears in the sanctions lists or caution advices circulated by Reserve Bank of India.
i. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
j. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
k. In the event the customer is permitted to act on behalf of another person/entity, the Company shall verify that the customer has the necessary authority to do so by scrutinizing the authorizing document/s.

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

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

Implementation of the Company's CAP should not become too restrictive and result in denial of the Company's services to general public, especially those who are financially or socially disadvantaged.

8.2. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

The Company prepares a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy. The customer profile contains the information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence depends on the risk perceived by the Company. At the time of credit appraisal of the applicant the details are recorded along with his profile based on meeting with the applicant (by the Company's representative) apart from collection of applicable documents and information as per the credit policy/products norms as may be in practice. However, while preparing customer profile, the Company seeks only such information from the customer which is relevant to the risk category and is not intrusive. Any other information from the customer should be sought separately with his/her consent and after opening the account. The customer profile will be a confidential document and details contained therein are not divulged for cross selling or for any other purposes. Further the Company shall allot Unique Customer Identification Number to each of its Customer.

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

a. Commencement of an account-based relationship with the customer.
b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. When a company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
d. The company will not seek introduction while opening accounts.
e. Where there is any update in the documents submitted for due diligence to the company, the customer shall submit such records within 30 days of such updation for the purpose of updating the records.

8.2.1. CUSTOMER DUE DILIGENCE PROCEDURE (CDD) IN CASE OF INDIVIDUALS

For undertaking CDD, the Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

a. the proof of possession of Aadhaar number where offline verification can be carried out;
b. the proof of possession of Aadhaar where offline verification cannot be carried out or any other OVD or the equivalent e-document thereof containing the details of his identity and address;

c. the KYC Identifier with an explicit consent to download records from CKYCR; and

d. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

e. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as instructed by the Company from time to time as per the credit policy of the company:

Where the customer has submitted,

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

ii. An equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annex 1.**

iii. any OVD or proof of possession of Aadhaar number under clause (b) above where offline verification cannot be carried out, the company shall carry out verification through digital KYC as specified under **Annex** 1. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

iv. KYC Identifier under clause (c) above, the RE shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government/RBI, instead of carrying out digital KYC, the company may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted. The Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer.

Explanation 1: The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

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

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

ii. Property or Municipal tax receipt;

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

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

Where the customer submits the above-listed documents as proof of address the Company shall ensure to collect the OVD (as specified in **Para 4.4** of the policy) with current address within a period of three months of submitting the above said documents.

Explanation 3: 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.

Explanation 4: In case of existing customers where the Permanent Account Number or equivalent e-document thereof or Form No.60 is not available, the 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. Before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Appropriate relaxations may be granted, on case-to-case basis, for continued operation of accounts for customers who are unable to provide Permanent Account Number or Form No. 60 owing to injury, illness, or infirmity on account of old age or otherwise, and such like causes. For the purpose of ceasing the operation of the account (loan), only credits shall be allowed.

Explanation 5: Where the OVD presented by a foreign national does not contain the details of address (in India), in such case the documents issued by the Government departments of foreign jurisdictions **and** letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address (in India). Both documents shall be collected in line with the RBI norms.

Explanation 6:

Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs)

In case a person who desires to open an account is not able to produce documents, as specified in **Para 8.2.1** above, the company may at their discretion open accounts subject to the following conditions:

a. The company shall obtain a self-attested photograph from the customer.
b. The designated officer of the company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
c. The account shall remain operational initially for a period of twelve months, during which CDD as per **Para 8.2.1** shall be carried out.
d. Balances in all their accounts taken together **shall not exceed rupees fifty thousand** at any point in time.
e. The total credit in all the accounts taken together **shall not exceed rupees one lakh 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.

Explanation: 7: As per the UIDAI notification dated 04.04.2019 (No. 13012/184/2019/Legal/UIDAI /No. 2 of 2019) **"Proof of Possession of Aadhaar"** referred in the KYC policy includes;

(a) **Aadhaar letter:** Issued by the Authority carries name, address, gender, photo, and date of birth details of the Aadhaar number holder.

(b) **Downloaded Aadhaar (e-Aadhaar)**: Carries name, address, gender, photo, and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

(c) **Aadhaar Paperless Offline e-KYC:** An XML document generated by the Authority containing name, address, gender, photo, and date of birth details of the Aadhaar number holder. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

(d) **Aadhaar Secure QR Code:** A quick response code generated by the Authority containing name, address, gender, photo, and date of birth details of the Aadhaar number holder. This is digitally

signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

8.2.2. CDD MEASURES FOR SOLE PROPRIETARY FIRMS

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out as explained under **Para 8.2.1** of this policy.

In addition to the above, **any two** of the following documents or the equivalent e-documents there of 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 and Informal Micro Enterprises (IMEs) with an Udyam Assist Certificate (URC) MSME for the purposes of PSL classification.
b. Certificate/license issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. CST/VAT/ GST certificate (provisional/final).
e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or 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.

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

Provided a contact point verification is undertaken and collect such other information as per the credit policy of the company and clarification as would 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.

Informal Micro Enterprises (IMEs) with an Udyam Assist Certificate (URC) shall be treated as Micro Enterprises under MSME for the purposes of Priority Sector Lending (PSL) classification.

8.2.3. CDD MEASURES FOR COMPANY

For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof or such other information as instructed by the Company from time to time as per the credit policy of the company shall be obtained:

a. Certificate of incorporation
b. Memorandum and Articles of Association
c. Permanent Account Number of the company
d. A resolution from the Board of Directors and power of attorney granted to its managers, officers, or employees to transact on its behalf.
e. The names of the relevant persons holding senior management position; and
f. The registered office and the principal place of its business if it is different.
g. CDD of the individual who is a beneficial owner, the managers, officers, or employees, as the case may be, holding an attorney to transact on the company's behalf shall be carried as explained under **Para 8.2.1** of this policy.

8.2.4. CDD MEASURES FOR PARTNERSHIP FIRM

For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof or such other information as instructed by the Company from time to time as per the credit policy of the company shall be obtained:

a. Registration certificate
b. Partnership deed
c. Permanent Account Number of the partnership firm
d. The names of all the partners and address of the registered office, and the principal place of its business, if it is different.
e. CDD of the individual who is a beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf shall be carried out as explained under **Para 8.2.1** of this policy.

8.2.5.(A) REGISTERING DETAILS OF NON-PROFIT ORGANIZATION (NPO) WITH DARPAN

Where the customer is an NPO, the details of the customer shall be registered on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a customer and the reporting entity has ended or the account has been closed, whichever is later.

8.2.5. CDD MEASURES FOR TRUST

For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof or such other information as instructed by the Company from time to time as per the credit policy of the company shall be obtained:

a. Registration certificate
b. Trust deed
c. Permanent Account Number or Form No.60 of the trust
d. The names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and
e. List of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust."
f. CDD of the individual who is a beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf shall be carried out as explained under **Para 8.2.1** of this policy.

8.2.6. CDD MEASURES FOR AN UNINCORPORATED ASSOCIATION OR A BODY OF INDIVIDUALS

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Resolution of the managing body of such association or body of individuals.
b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.
c. Power of attorney granted to transact on its behalf.
d. CDD of the individual who is a beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf shall be carried out as explained under **Para 8.2.1** of this policy.
e. Such information as may be required by the Company as per credit policy of the company to collectively establish the legal existence of such an association or body of individuals.

Explanation 1: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

Explanation 2: Term 'body of individuals' includes societies.

8.2.7. CDD MEASURES FOR JUDICIAL PERSONS NOT SPECIFICALLY COVERED IN THE EARLIER PART

For opening accounts of persons who purports to act on behalf of a juridical person or individual or trust" not specifically covered in the earlier part, such as societies, universities and local bodies like

village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

a. Document showing name of the person authorised to act on behalf of the entity;
b. CDD of the individual holding an attorney to transact on its behalf shall be carried as explained under **Para 8.2.1** of this policy and
c. Such documents as may be required by the company as per the credit policy of the company to establish the legal existence of such an entity/juridical person.

8.2.8 IDENTIFICATION OF BENEFICIAL PERSON:

For opening an account of a **Legal entity** as specified in **Para 8.2.3 to 8.2.7** who is not a natural person, all reasonable measures in terms of sub-rule (3) of Rule 9 of PML (Maintenance Of Records) Rules 2005 shall be undertaken to identify the "beneficial owner" keeping in view of the following:

i) Where the customer or the owner of the controlling interest is
   a. an entity listed on a stock exchange in India, or
   b. it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
   c. 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.

ii) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Beneficial Owner (BO)" means;

i) Where the customer is a **company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a **controlling ownership interest** or who exercise **control** through other means.

   Explanation- For the purpose of this sub-clause-

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

   "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.

ii) Where the customer is a **partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than **15 per cent** of capital or profits of the partnership.

iii) Where the customer is an **unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have 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: 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.

iv) Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with **10 per cent 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.

8.2.9 VIDEO BASED CUSTOMER IDENTIFICATION PROCEDURES

The Company may undertake V-CIP to carry out:

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

Provided that in case of CDD of a proprietorship firm, the company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 and Section 29, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17 of RBI KYC Master Directions.

iii) Updation/Periodic updation of KYC for eligible customers

While undertaking V-CIP, following minimum standards shall be adhered to:

(a) V-CIP Infrastructure

i) Adherence to the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any

technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE only and all the data including video recording is transferred to the RE's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed but not later than 3 days and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

ii) 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 consent should be recorded in an auditable and alteration proof manner.

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

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

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

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

vii) 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 empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservices shall 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/ regulatory guidelines.

(b) V-CIP Procedure

i) The Company shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) If there is a disruption of any sort including pausing of video, reconnecting calls, etc., it should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated. iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

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

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

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

- Offline Verification of Aadhaar for identification
- KYC records downloaded from CKYCR, in accordance with Section 56 of RBI KYC Master directions, using the KYC identifier provided by the customer.
- Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of RBI KYC Master Directions.

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

Further, in line with the prescribed period of three 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 three working days of downloading / obtaining the identification information through CKYCR / Aadhaar

authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, it shall be ensured that no incremental risk is added due to this.

vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

viii) 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.

ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

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

xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank. (The option is not available for NBFCs).

xii) 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.

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the technical/IT team of the company.

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. It shall be ensured that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

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

8.2.10 SCREENING OF ACCOUNTS WITH THE LISTS CIRCULATED BY THE UNITED NATIONS SECURITY COUNCIL (UNSC)

It shall be ensured that there is not any account in the name 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). Details of accounts resembling any of the individuals/entities (confirmed with reasonable suspicion) in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under Unlawful Activities (Prevention) (UAPA) Act, 1967.

9. RISK MANAGEMENT

The Company shall have a risk-based approach which includes the following.

a. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perceptions.

b. Broad principles are laid down by the company for risk-categorization of customers.

c. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

d. 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.

   The authorised persons carrying out due diligence and collecting various information based on the perceived risk of the customer shall ensure that the process is non-intrusive.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI and other agencies, etc., may also be used in risk assessment.

10. CUSTOMER DUE DILIGENCE BY THIRD PARTY

The Company may engage a third party to do Customer Due Diligence and verifying the identity of customers at the time of commencement of an account-based relationship, 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 Central KYC Records Registry.
b. Adequate steps are taken by the Company to satisfy that copies of identification data and other relevant documentation relating to the customer due diligence requirements are made available from the third party upon request without delay.
c. The third party is regulated, supervised, or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
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.

11. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions, or delivery channels, etc.
b. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.
c. The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.
d. The outcome of the exercise shall be put up to the Risk Management Committee on a quarterly basis and will be available to competent authorities and self-regulating bodies.

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

12. ONGOING DUE DILIGENCE/MONITORING OF TRANSACTIONS

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

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

b. Transactions which exceed the thresholds prescribed for specific categories of accounts.

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

The extent of monitoring shall be aligned with the risk category of the customer. High risk accounts have to be subjected to more intensified monitoring. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

13. PERIODIC UPDATION

The Company shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out **at least once in every two years for high-risk customers**, **once in every eight years for medium risk customers** and **once in every ten years for low-risk customers** from the date of opening of the account / last KYC updation. In line with RBI direction the requirement is being documented as part of the KYC Policy.

a) Individual Customers:

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

ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (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.

Further, the Company as an option may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation. As per RBI the option shall be as specified in the KYC Policy.

iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the respective departments/operations department. Wherever required, the company may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.

iv. **Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation**. To clarify, conditions stipulated in Para 17 of the KYC Master Directions are 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. REs 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.

b) Customers other than individuals:

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

ii. **Change in KYC information:** In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new LE customer.

c) **Additional measures:** In addition to the above, it shall be ensured that,

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

ii. Customer's PAN details, if available with the Company, are verified from the database of the issuing authority at the time of periodic updation of KYC.

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

iv. In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch, as per the terms captured in this policy as per the RBI directions.

v. The Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be as per the terms captured in this policy in line with the RBI directions.

vi. The Company shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

vii. The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Company's end.

14. ENHANCED DUE DILIGENCE

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

shall be undertaken by the Company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

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

14.2. Accounts of Politically Exposed Persons (PEPS):

The Company shall 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 a senior level in accordance with the company's Customer Acceptance Policy;
d. all such accounts are subjected to enhanced monitoring on an on-going basis;
e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

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

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

14.3. Client Accounts Opened by Professional Intermediaries:

The Company shall ensure while opening client accounts through professional intermediaries, that:

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

b. The Company shall not open accounts of such professional intermediaries who are bound by any client.

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

d. The ultimate responsibility for knowing the customer lies with the Company.

15. MAINTENANCE OF RECORDS OF TRANSACTIONS

The Company shall maintain proper records of the transactions as required under the provisions of PML Act and Rules. The Company shall;

a. Maintain all necessary records of transactions between the Company and the customer, for at least five years from the date of transaction or any other higher periods specified in any other law.

b. 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. make available swiftly, the identification records and transaction data to the competent authorities upon request;

d. Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005)

e. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 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. Have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

g. 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.

   For the purpose of this Section, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

h. The company has framed a document retention policy in order to ensure that the above requirements are adhered.

15A. IMPLEMENTATION OF POLICIES BY GROUPS

The Group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003) shall be implemented by the group companies .

16. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA (FIU-IND)

The Company shall furnish the following reports to the Financial Intelligence Unit-India (FIU-IND), with regard to information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof, in the manner so specified and within the timelines prescribed therein;

a. Cash Transactions Report (CTR)
b. Suspicious Transactions Report (STR)

The company is registered with FIU-IND . The company submits Cash transaction report (CTR) monthly and Suspicious Transaction Report (STR) on identification of such transaction with FIU-IND.

The company has implemented a system not to accept any cash of **more than Rs. 2 lakhs** from its borrowers. Hence, it normally does not and would not have large cash transactions. However, if and when cash transactions of Rs.10 lakhs and above are undertaken, the company will keep proper record of all such cash transactions in a separate register maintained at its office.

The company monitors transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the Company depends on the risk sensitivity of the account and special attention is given to all complex unusually large transactions, which have no apparent economic or lawful purpose.

The company shall promptly report such high value cash transactions or transactions of a suspicious nature to the appropriate regulatory and investigating authorities. The company has the system of throwing alerts on inconsistent transactions and profile of the customers is updated for effective identification and reporting of suspicious transactions.

17. CONFIDENTIALITY OF INFORMATION

Information collected from customers for the purpose of opening of account shall be treated as confidential and in accordance with the agreement/terms and conditions signed by the customers. The information collected from customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer. While considering the requests for data/information from Government and other agencies, banks 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 banking transactions.

The exceptions to the said rule shall be as under:

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

18. CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company shall capture the KYC information for sharing with the CKYCR in the manner as specified for individuals and legal entities in the RBI KYC Master Directions. 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. As per the directions NBFCs shall upload the KYC data pertaining to all **"new individual accounts"** opened on or after from April 1, 2017, and **"legal entities"** opened on or after April 01, 2021, with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

In line with the directions, in order to ensure that all KYC records are incrementally uploaded on to CKYCR, the company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates at the time of periodic updation as specified in **Para 14** of this policy, or earlier, when the updated KYC information is obtained/received from the customer.

Once KYC Identifier is generated by CKYCR, the company shall ensure that the same is communicated to the individual/Legal Entity as the case may be.

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 –

i. there is a change in the information of the customer as existing in the records of CKYCR;

ii. the current address of the customer is required to be verified;

iii. 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.

iv. the validity period of documents downloaded from CKYCR has lapsed.

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

The Taxation Dept of the Company shall ensure adherence to the provisions of Income Tax Rules 114F, 114G and 114H and comply with the reporting requirements as prescribed under the FATCA and CRS norms, including, developing of Information Technology (IT) framework for carrying out due diligence procedure and developing a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

A "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary shall be constituted to ensure compliance.

20. REQUIREMENTS / OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS / COMMUNICATION IS FROM INTERNAL AGENCIES

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

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

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

ii. 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 meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).
b. The company shall not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
c. The Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
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 Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. The Director of FIU-India has been designated as the CNO. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. The Company shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.
e. The Company may 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 CNO without delay.
g. In case an order to freeze assets under Section 12A is received by the REs from the CNO, the Company shall, without delay, take necessary action to comply with the Order.
h. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by the Company along with full details of the asset frozen, as given by the applicant, to the CNO within two working days.

The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities ', to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on

Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, other UNSCRs, lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

Adequate attention shall be paid by the Company to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

21. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

The Company shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and also should have an ongoing employee training programs so that members of the staff are adequately trained in KYC/AML/CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/staff dealing with new customers so that all concerned fully understand the rationale behind the KYC policies and implement them consistently.

22. ADHERENCE TO KNOW YOUR CUSTOMER (KYC) GUIDELINES BY NBFCS AND PERSONS AUTHORISED BY NBFCS INCLUDING BROKERS/AGENTS ETC.

Persons authorised by NBFCs and their brokers/agents **or the like**, shall be fully compliant with the KYC guidelines applicable to NBFCs.

All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs including brokers/agents etc. who are operating on their behalf.

The books of accounts of persons authorised by NBFCs, including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

23. INTRODUCTION OF NEW TECHNOLOGIES

The Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products, and shall further 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.

24. REPOTING TO CREDIT BUREAU

The company shall ensure that the following while Furnishing of Credit Information to Credit Information Companies (CICs):

a. The records submitted to CICs are updated regularly and no instances of repayment, including that of the last instalment, are left unreported.
b. To have nodal officers for dealing with CICs
c. Customer grievance redressal should be given top priority especially in respect of complaints relating to updating/alteration of credit information.
d. Grievance redressal in respect of credit information should be integrated with the existing systems for grievance redressal. Aspects relating to customer grievances pertaining to credit information are an integral part of customer service policy.
e. To abide by the period stipulated under Credit Information Companies (Regulation) Act, 2005 (CICRA) and the Rules and Regulations framed thereunder in respect of updating, alteration of credit information, resolving disputes, etc. Procedure prescribed under Rule 20 and 21 of the Credit Information Companies Rules, 2006 in this regard should be adhered to. Deviations from stipulated time limits should be monitored and commented upon in the periodical reports/reviews put up to the Board/Committees of Board on customer service.
f. Updating of credit information should take place on a monthly basis or at such shorter intervals as may be mutually agreed upon between the company and the CIC.
g. To provide full customer information to the CICs.
h. To mandate the usage of CIRs in their credit appraisal process.
i. First time borrowers' loan applications should not be rejected just because they have no credit history.
j. Banks/FIs and CICs should ensure that the credit records of borrowers are regularly updated by banks/FIs and that issues such as where repayment of the last instalment of a loan does not get reported does not arise.
k. Banks/FIs and CICs should have a structured process of complaint redressal.

25. PHONE NUMBER CHANGE PROCESS – OTP BASED

The phone number change shall be on One time Pin (OTP) based process, and the channels of requesting for the number change shall be through **Phone, WhatsApp, Chatbot & Saathi App.**

25.1 Channel - 'Phone':

The below process is followed at the Call Centre to change customer's registered mobile number.

a. **If customer called the customer care from his registered mobile number:**
   Agent will trigger OTP to both old and new mobile number for Phone number change. When both the OTP is validated, new number would be automatically changed in CRM & RMS both. In data mart the changes would be reflected by end of the day.
b. **Customer calls customer care from non-registered mobile number:**
   i. Customer care agents will check with the customer whether the registered number is working or not.
      - If customer confirms as the registered mobile number is working - Then customer is requested to call us back from his registered mobile number.
      - If customer confirms registered number is not working - Then agent shall inform the customer to send the phone number change request with the self-attested KYC through email / letter.

   ii. On receipt of the request with self-attested KYC, our agent shall verify the KYC and update new phone number in system with OTP validation to new mobile number. In case of KYC mismatch, customer is updated on the reason and guided to provide the valid document for further process.
   iii. In data mart the changes would be reflected by end of the day.

25.2. Channel WhatsApp, Chatbot & Saathi App:

The below process is followed when customer wants to change the registered mobile through WhatsApp /Chat bot.

a. Customers need to choose the menu Phone number change.
b. System will ask the customer if he wants to change his registered mobile and if he changes, then only new number will be active and will no longer be able to use old number.
c. On customer confirmation to continue, OTP will be triggered to his registered mobile number.
d. Customer should input the OTP and upon validation customer is asked to enter his new mobile number.
e. OTP will be triggered to his new mobile number.
f. On successful OTP validation, new Mobile number gets updated in his loan account in RMS & CRM.
g. In data mart the changes would be reflected by end of the day.

****

Annex 1

Digital KYC Process

A. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of customers and the KYC process shall be undertaken only through this authenticated application of the Company.

B. The access of the Application shall be controlled by the Company, and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice-versa. The original OVD shall be in possession of the customer.

D. The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall 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 white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled out as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is

available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the Company shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the 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.

…….