CHARTERED FINANCE & LEASING LTD. (CFL)

("NBFC/ B-13.02480")

SUMMARY OF POLICY

Particular	Details
Policy Name	KYC AML Policy
Version	V3
Latest Approval/Review Date	20-May-2025
Review Cycle	Annually
Approver	Board of Directors of Chartered Finance & Leasing Ltd

VERSION HISTORY

VERSION NO.	APPROVAL	VERSION DESCRIPTION	REGULATORY REFERENCE	REMARKS
I	01-May-2016	2016	RBI Regulation	Policy adopted by the Board
II	07-Apr-2022	2022	RBI Regulation	Reviewed by Board
III	20-May-2025	2025	RBI Regulation	Reviewed by Board

KYC AML Policy

Contents

1. Introduction

As per the guidelines issued by RBI vide its Master Direction "Know Your Customer (KYC) norms/ Anti-Money Laundering (AML) standards/ Combating Financing of Terrorism (CFT)/ Obligation of banks and financial institutions under PMLA, 2002" the Company has in place a Policy on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards.

The Know Your Customer (KYC) guidelines have been updated in accordance with the recommendations proposed by the Financial Action Task Force (FATF) with regards to Anti Money Laundering (AML) measures and Combating Financing of Terrorism (CFT).

This Policy shall be termed as KYC & AML policy of Chartered Finance & Leasing Ltd (hereinafter referred to as "Company" or "CFL").

This Policy lays down the guidelines to be followed by the Company for Customer Identification Procedure while opening an account. It also prescribes measures to be undertaken by the Company for monitoring suspicious transactions in order to report the same to an appropriate authority.

This policy uniformly applies to all customers of the Company (Asset, Third Party Products, Walk-in Customers), irrespective of their relationship with the Company.

2. Guiding Principles

The objective of this policy is to prevent the Company from being used, intentionally or unintentionally, for money laundering or terrorist financing activities by criminal elements.

KYC norms shall provide the company with a better understanding of its customers and their financial dealings which shall help in managing their risks more carefully.

This Policy shall also allow the company to monitor and report any suspicious transactions in accordance with the relevant regulatory guidelines.

3. Definitions

i. "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);
ii. "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.
iii. "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
iv. Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

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

2. "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.

a. 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 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

b. 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.

c. Where the **customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. Certified Copy" - Obtaining a certified copy by CFL 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.

vi. "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.

vii. “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. The Company shall nominate the Managing Director or a whole-time Director, duly authorized by the Board of Directors, as the “Designated Director”. In no case, the Principal Officer shall be nominated as the “Designated Director”.

viii. “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.

ix. “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).

x. “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.

xi. “Group” means the term “group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961)

xii. “Know Your Client (KYC) Identifier” means the unique number or code assigned to a customer by the Central KYC Records Registry.

xiii. “Non-profit organisations” (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

xiv. Officially Valid Document (OVD)

A. The documents which are mandatorily required and valid for initiating an account opening process are called Officially Valid Documents. These include:
    a) Passport
    b) Driving License
    c) Voter’s Identity Card issued by the Election Commission of India
    d) Aadhar Card / proof of possession of Aadhar Number
    e) Job Card issued by NREGA duly signed by an official of State Government

f) Letter issued by National Population Register containing details of name, address
g) Any other document as notified by the Central Government in consultation with the Reserve Bank of India

B. In case the OVD furnished by the customer does not contain updated/ current address, the following documents or the equivalent e-documents thereof 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 license agreements with such employers allotting official accommodation;

C. customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

xv. "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).

xvi. "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. 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 (a to e), and
   g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvii. "Principal Officer" means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

xviii. "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.

xvii. "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.

xix. "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 this Master Direction.

xx. "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.

xxi. "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.

xxii. “Walk-in Customer” means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.

xxiii. “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

xxiv. “Customer identification” means undertaking the process of CDD.

xxv. “FATCA” means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

xxvi. “IGA” means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

xxvii. “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

xxviii. “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the RE or meeting the officials of RE.

xxix. “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that those are consistent with RE’s knowledge about the customers, the customers’ business and risk profile, the source of funds/wealth.

xxx. “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.

4. Know Your Customer (KYC) Policy

Why "Know your Customer"?

One of the best methods of preventing and preventing money laundering is acquiring a sound knowledge of customers' business and pattern of financial transactions. Adoption of procedures by company to know their customers is not only a principle of good business but also an essential tool to avoid involvement in money laundering. The company shall adopt appropriate KYC procedures and internal control measures to:

a) Determine and document the true identity of the customers who establish relationships, open accounts or conduct significant business transactions, and obtain basic background information on customers.

b) Assess the money laundering risk posed by customers' expected use of Company's products and services.

c) Protect the company from the risks of doing business with any individual or entity whose identity cannot be determined or who refuses to provide information or who has provided information that contains significant inconsistencies which cannot be resolved after due investigation.

d) Ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

e) Ensure to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003). Accordingly, every RE which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

In accordance with the RBI guidelines, the KYC policy shall have the following four main elements:

a) Customer Acceptance Policy (CAP)
b) Customer Identification Procedure (CIP)
c) Risk Management
d) Monitoring of Transactions

4.1 Customer Acceptance Policy (CAP)

As per the RBI guidelines, the company shall follow below mentioned Customer Acceptance Policy which prescribes the following set of guidelines: -

a. No account is opened in anonymous or fictitious/benami name.
b. No account is opened where the company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The RE shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
c. No transaction or account-based relationship is 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, as specified.
e. 'Optional'/additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer.
f. Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account or avail any other product or service from the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in KYC Master Directions issued by RBI. Further, company shall also scan existing active customers against RBI published sanctions list.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
k. Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
l. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

Provided that above shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
Provided further that where RE forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

4.2 Customer Identification Procedure (CIP)

4.2.1 The Company shall follow recommendations issued under the RBI Master Direction containing the Customer Identification Procedure to be carried out at various stages. The Company shall follow Customer Identification Procedure while/whenever:

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

4.2.2 For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, RE, shall 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 immediately from the third party or from the Central KYC Records Registry.
b) Adequate steps are taken by RE to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under 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 RE.

4.3 Risk Management

4.3.1 For Risk Management, 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 perception of the company. This categorization shall be based on the customer type (Individual/ Non-Individual) (Annexure C), industry to which they belong (Annexure D). Further methodology to be followed for risk categorization is given in Annexures C, D.
b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

   Provided that various other information collected from different categories of customers relating to the perceived risk is non-intrusive and the same is specified in the KYC policy.

c) The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
d) The Company shall have a system relating to periodic review of risk categorization of the customers. The Company shall ensure that the risk category of customers is reviewed with a periodicity of not more than 6 months. The Company shall be undertaking a review of all those accounts existing as on September 30 and March 31 every year which were opened at least six months prior to these review dates – thus giving a vintage of at least six months to each account being reviewed.

4.3.2 Updation/Periodic Updation of KYC

REs shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk. However, 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.

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 RE, customer's mobile number registered with the RE, digital channels (such as mobile application etc), 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 RE, customer's mobile number registered with the RE, ATMs, digital channels (such as mobile application etc), 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, company, at their option, 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 updation / periodic updation.

iii) Aadhaar OTP based e-KYC in non-face to face mode may be used for updation / periodic updation. 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.

Risk-based approach with respect to periodic updation of KYC (Individual)

Risk Categorization	**Periodic Update**	**Change in KYC/CDD**	**Documents**
Low Risk	Every 10 years	No Change in KYC-	Self-Declaration
		Change in Address	Self-Declaration to be verified through positive confirmation
Medium Risk	Every 8 Years	No Change in KYC-	Self-Declaration with copy of OVD
		Change in Address	Self-Declaration with copy of OVD to be verified through positive confirmation
High Risk	Every 2 years	No Change in KYC-	Self-Declaration with copy of OVD

		Change in Address	Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

b) **Customers other than individuals:**

i) **No change in KYC information:** In case of no change in the KYC information of the 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 company), letter from an official authorized by the LE in this regard, board resolution etc. Further, company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii) **Change in KYC information:** In case of change in KYC information, 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, company shall ensure 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, 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, is 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 updation / periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation / 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, company may consider making available the facility of updation / periodic updation of KYC at any branch.

v) 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.

vi) In case of existing customers, RE 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 RE 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 RE shall give the customer an accessible notice and a reasonable opportunity to be heard.

d) RE 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 REs 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 REs' end.

e) Due Notices for Periodic Updation of KYC

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

4.3.3 Enhanced Due Diligence

a) **Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding** (other than Aadhaar OTP based on-boarding**):** Non-face-to-face onboarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by REs for non-face-to-face customer onboarding (other than Aadhaar OTP based on-boarding):

i) In case RE 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.

ii) 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. RE shall

have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

iii) Apart from obtaining the current address proof, RE 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.

iv) RE shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

v) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

vi) 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.

b) Accounts of Politically Exposed Persons (PEPs) :

REs shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

(i) REs have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

(ii) Reasonable measures are taken by the REs for establishing the source of funds / wealth;

(iii) the approval to open an account for a PEP shall be obtained from the senior management;

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

(v) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

These instructions shall also be applicable to family members or close associates of PEPs.

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

c) Client accounts opened by professional intermediaries: RE shall ensure while opening client accounts through professional intermediaries, that:

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

ii) REs shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

iii) REs shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the RE.

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

v) REs 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.

4.4 Customer Due Diligence (CDD) Procedure

4.4.1 Individuals

A) For undertaking CDD, REs 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:

1. the Aadhaar number where, he decides to submit his Aadhaar number voluntarily to RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or
2. the proof of possession of Aadhaar number where offline verification can be carried out; or
3. the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address **(As per List below)**;
4. the KYC Identifier with an explicit consent to download records from CKYCR and
5. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
6. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE:

Provided that where the customer has submitted,

a. Aadhaar number under clause (1) above RE shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.
b. Proof of possession of Aadhaar under clause (2) above where offline verification can be carried out, the RE shall carry out offline verification.
c. An equivalent e-document of any OVD, the RE 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 Annexure A .

d. Any OVD or proof of possession of Aadhaar number under clause (3) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC as specified under Annexure A.
e. KYC Identifier under clause (4) above, the RE shall retrieve the KYC records online from the CKYCR in accordance with paragraph 8.
Provided that RE may at there option instead of carrying out digital KYC, shall 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.

Explanation 1: RE shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (a) above.
Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.
Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder

List of documents required as proof of Identity & proof of address: -

For Individuals :-

i) **Proof of Identity**:
Any of the following documents or the equivalent e-document are valid/acceptable as the proof of identity:

Officially Valid Documents:
a) Passport
b) Driving License
c) Voter's Identity Card issued by the Election Commission of India.
d) Job Card issued by NREGA duly signed by an official of State Government.
e) Letter issued by National Population Register containing details of name, address.
f) Aadhar Card / Proof of possession of Aadhar*
* Proof of Possession of Aadhar as mentioned above shall cover any of the following documents:

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

- 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.
- 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.

The Aadhaar number holder can use any of the documents mentioned above to prove possession of Aadhaar number, subject to the Company's right to verify the genuineness of the above-mentioned documents.

ii) **Proof of Address**

Any of the following documents or the equivalent e-document are valid/acceptable as the proof of address:

a) Passport
b) Driving License
c) Voter's Identity Card issued by the Election Commission of India.
d) Job Card issued by NREGA duly signed by an official of State Government.
e) Letter issued by National Population Register containing details of name, address.
f) Aadhar Card / Proof of possession of Aadhar*

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 2 months old from the date of application of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
b) Latest Property or Municipal Tax receipt
c) Pension or family pension payment orders (PPOs) issued to retired central/state government employees
d) Letter of allotment of accommodation/leave and license agreements allotting official accommodation issued by relevant bodies. (Ex. State/Central Government, Statutory or Regulatory Bodies, Public Sector Undertakings, Scheduled Commercial Banks, Financial Institutions and Listed companies).

Provided further that the customer shall submit Aadhaar/ OVD updated with current address within a period of three months of submitting the above documents.

For the limited purpose of current address proof, a self-declaration from customer shall be a permissible as proof of current address who opened their account through e-authentication (OTP and Biometric) mode of KYC.

Note: PAN/ Form 60 is required to be obtained mandatorily from the customer.

For Married Women Accounts:

In case the identity proof of post marriage name is not available with customer the following documents shall be collected:

a) Marriage Certificate issued by the State Government or Gazette notification indicating change in name/ Affidavit.
b) Certified copy of the 'officially valid document' in the existing name as proof of address and identity
c) ID proof of husband.
d) 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.

Notes: -

a) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents.
b) All the KYC documents to be self-certified by the customer.
c) Customer to sign across the photograph pasted on the Account Opening Form with signatures running both on to Account Opening Form and the photograph.
d) Customer to sign the Account Opening Form (AOF) in the presence of a Company official and the Company official to certify the AOF with a notation 'Customer Signed in my presence' under his signature and employee number.
e) In case the identity information submitted by the customer does not have current address of the customer, the customer shall submit additional document as a proof of current address.

B) REs may undertake V-CIP as per procedure and other requirements mentioned in Annexure B to carry out:
   a) 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, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in paragraph 4.4.2, apart from undertaking CDD of the proprietor.

b) Updation/Periodic updation of KYC for eligible customers.

4.4.2 Sole Proprietorship: -

Apart from Customer Identification Procedure as applicable to the Proprietor, any two of the following documents or the equivalent e-documents in the name of the proprietary concern shall suffice as Proof of Existence:

a) Registration certificate issued by Central government, State governments, local bodies and statutory authorities including Udyam Registration Certificate (URC) issued by the Government.
b) Certificate/license issued by the Municipal authorities under Shop & Establishment Act
c) Sales and income tax returns
d) CST/VAT/Goods and Service Tax (GST) Certificate (Provisional / Final)
e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
f) Complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor reflecting the firm's income, duly authenticated/acknowledged by the IT authorities.
g) Utility bills such as electricity, water, and landline telephone bills
h) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute

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) One-month account statement from existing bank account maintained with a scheduled commercial bank having at least one customer-initiated transaction and not more than 4 months old.
c) Property or Municipal Tax receipt
d) Rent agreement/ Sale deed with site verification report.

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

Provided RE undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall

confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Notes:

a) Registration Certificate should carry a) Name of the Firm b) Name of the Proprietor c) Address of the Firm
b) In case the document submitted as proof of existence contains both proof of existence and proof of address, no separate proof of address is required to be furnished.
c) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents
d) All the KYC documents to be certified under full signature and stamp.
e) Customer to sign across the photograph pasted on the Account Opening Form with signatures running both on to Account Opening Form and the photograph.

4.4.3 Partnership Firms: -

For opening an account of a partnership firm, Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

Proof of Existence

a) Registration certificate issued by government authorities
b) Partnership deed
c) Permanent Account Number of the partnership firm and
d) Documents, as specified in paragraph 4.4.1, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
e) The names of all the partners and
f) Address of the registered office, and the principal place of its business, if it is different.

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) PAN intimation letter
c) Property or Municipal Tax receipt
d) One-month account statement from existing bank account maintained with a scheduled commercial bank having at least one customer-initiated transaction and not more than 4 months old.
e) Rent agreement/ Sale deed with site verification report
f) Registration certificate issued by Central government, State governments, local bodies or statutory authorities having address

Notes:

a) Unregistered partnership firms shall be included under the term 'Unincorporated Association/AOP'.

b) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.

c) The Company shall identify and obtain proof of identity & address of Beneficial owners. 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 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

Note: Where the Company is unable to identify the natural person (as mentioned above), the identity of the relevant natural person who holds the position of senior managing official to be recorded with proof of identity and address.

d) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents

e) All the KYC documents to be certified under full signature and stamp.

f) Proof of address of principal place of business will be required if it is different from registered office.

4.4.4 Companies (Private/ Public/ One Person Company): -

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

Proof of Existence

a) Certificate of incorporation
b) Memorandum and Articles of Association
c) Board Resolution – duly signed to its managers, officers or employees to transact on its behalf
d) Permanent Account Number of the company
e) Documents, as specified in paragraph 4.4.1, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
f) The names of the relevant persons holding senior management position; and
g) The registered office and the principal place of its business, if it is different.

Proof of Address (for both Mailing and Registered Office Address)

a) Certificate of registration under any statute/ act or professional bodies
b) Any registering/ licensing document issued by central government or state govt. authority

c) Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)
d) PAN intimation letter
e) INC-22 or Form 18 along with ROC challan
f) Rent agreement/ Sale deed with site verification report

Notes:

a) The Company shall identify and obtain proof of identity & address of Beneficial owners. The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more judicial persons, has a controlling ownership interest. (ownership of more than 10% of the shares or capital or profits of the company).

   Note: Where the Company is unable to identify the natural person (as mentioned above), the identity of the relevant natural person who holds the position of senior managing official to be recorded with proof of identity and address.

b) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.
c) Board resolution can be signed by Managing Director or CRO or at least two directors. A director cannot authorize himself for doing all necessary acts required in relation with operating of Company account. However, if BR is signed by one director including MD, then it can be considered.
d) The original of all documents should be sighted by the Company official and the notation “Original Seen and Verified” under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents
e) All the KYC documents to be certified under full signature and stamp.
f) Proof of address of principal place of business will be required if it is different from registered office.
g) The expression "senior management" means personnel of the company who are members of its core management team excluding Board of Directors comprising all members of management one level below the executive directors, including the functional heads.

4.4.5 Trusts: -

Certified copy of each of the following documents or the equivalent e-documents thereof is required to be submitted:

Proof of Existence

a) Registration Certificate issued by Government Authorities/registrar of trusts/ assistant charity commissioner
b) Trust deed

c) Resolution to open and operate the Company account. Resolution should clearly indicate the authorized signatories.
d) PAN card in the name of the Trust
e) Documents, as specified in paragraph 4.4.1, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
f) The names of the beneficiaries, trustees, settlor protector, if any and authors of the trust
g) The address of the registered office of the trust; and
h) List of trustees and documents, as specified in paragraph 4.4.1, for those discharging the role as trustee and authorised to transact on behalf of the trust.

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) PAN intimation letter
c) Property or Municipal Tax receipt
d) One-month account statement from existing bank account maintained with a scheduled commercial bank having at least one customer-initiated transaction and not more than 4 months old.
e) Communication from Registrar/ Ministry of Home affairs
f) Rent agreement/ Sale deed with site verification report
g) Registration certificate issued by Central government, State governments, local bodies or statutory authorities having address

Note:

a) If the account opening is in the name of a school/ college/ hospital/ unit of the trust, then following documents should be taken:
    1. Legally constitutional documents of trust such as Trust Deed should be obtained together with such other documents as required by KYC policy resolution of trustees approving Account in the name of individual school/ college/ hospital/ unit of the trust.
    2. Entity document issued in the name of school/ college/ hospital/ unit of the trust. If the entity is a pre-primary or nursery school, which need not be affiliated to any Board as per the law in force in the state concerned, the entity proof need not be insisted upon. In such cases the account would be opened as a unit of the parent entity. (School – Unit of Society/ Trust)
    3. Relationship proof between the trust and school/ college/ hospital/ unit of the trust
    4. Site verification Report (SVR) for the school/ college/ hospital/ unit of the trust by any Company Official

b) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.

c) Identity proof is required for every person signing any document on behalf of the trust.

d) The Company shall obtain the Beneficial ownership details / list of trustees shall be obtained. The ultimate beneficial owner (natural person) to be identified which would include author of the trust, the trustees and beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate control over the trust through a chain of control or ownership. Proof of identity and address of author/trustee/beneficiaries to be obtained.

e) In case of mismatch in list of Trustees mentioned in the constitutional documents with the current list of Trustees while account opening, following documents to be obtained:

- Letter of intimation of appointment of new trustee to charitable commissioner/ registrar of Trusts/ Income Tax Department OR
- Letter of Indemnity mentioning the current lists of Trustees to be obtained from the trust

f) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents

g) All the KYC documents to be certified under full signature and stamp.

Provided that in case of a trust, the RE shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of sub clause 4.2.1 of clause 4.2 of this policy.

4.4.6. Limited Liability Partnership (LLP): -

For opening an account of an LLP, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

Proof of Existence:

a) LLP Agreement
b) Certificate of Incorporation
c) PAN Card of LLP
d) List of all the partners including designated partners of LLP along with designated partner identification number – to be duly Verified from the Site
e) LLP declaration/resolution signed by at least 2 designated partners
f) Documents, as specified in paragraph 4.4.1, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
g) Address of the registered office, and the principal place of its business, if it is different.

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) One-month account statement from existing bank account maintained with a scheduled commercial bank having at least one customer-initiated transaction and not more than 4 months old.
c) PAN intimation letter of the LLP
d) Municipal Registration Certificate
e) Local Sales Tax/ Central Sales Tax License
f) CST/VAT/Goods and Service Tax (GST) Certificate (Provisional/ Final)
g) Import/ Export Certificate in the name of LLP
h) Property or Municipal Tax receipt
i) Rent agreement/ Sale deed with site verification report.
j) Registration certificate issued by Central government, State governments, local bodies or statutory authorities having address

Note:

a) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.
b) The Company shall identify and obtain proof of identity & address of Beneficial owners. 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 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

Note: Where the Company is unable to identify the natural person (as mentioned above), the identity of the relevant natural person who holds the position of senior managing official to be recorded with proof of identity and address.

c) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents
d) All the KYC documents to be certified under full signature and stamp.
e) Proof of address of principal place of business will be required if it is different from registered office.

4.4.7. Hindu Undivided Family (HUF): -

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

Proof of Existence:

a) HUF declaration duly signed by all adult co-parceners and naming the Karta, who would be authorized to operate the account
b) Karta's identity, signature and address proof as applicable for KYC of individuals
c) HUF Deed (if available)
d) PAN in the name of HUF

Proof of Address:

a) KYC as applicable to resident individual account and authorized signatories to the account.

Note:

a) In case the document submitted as proof of existence contains both proof of existence and proof of address, no separate proof of address is required to be furnished.
b) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents
c) All the KYC documents to be certified under full signature and stamp.

4.4.8 Societies/ Associations / Clubs: -

For opening an account of a Societies/ Associations / Clubs, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

Proof of Existence:

a) Certified copy of the certificate of registration of the society signed by MD/ Executive Director/ Member of the managing committee
b) Certified copy of bye-laws signed by the MD/ Executive Director/ Member of the managing committee
c) PAN Card in the name of society/ club/ association
d) Certified copy of the resolution to open the account signed by the
e) Society memorandum of association and rules and regulations
f) Documents, as specified in paragraph 4.4.1, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

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) One-month account statement from existing Company account maintained with a scheduled commercial Company having at least one customer-initiated transaction and not more than 4 months old.
c) PAN intimation letter of the Societies/ Clubs/ Associations
d) Registration Certificate
e) Any of the entity proof document mentioned above can also be accepted as an address proof if said document contains address.
f) Property or Municipal Tax receipt
g) Rent agreement/ Sale deed with site verification report

Note:

a) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.
b) The Company shall identify and obtain proof of identity & address of Beneficial owners. 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 Societies/ Associations / Clubs.
   Note: Where Company is unable to identify the natural person (as mentioned above), the identity of the relevant natural person who holds the position of a senior managing official to be recorded with proof of identity and address.
c) If the account opening is in the name of a school/ college/ hospital/ unit of the society, then the following documents should be taken
   - Legally constitutional documents of society should be obtained together with such other documents as required by KYC policy for opening account along with the resolution of members of the society approving opening of account in the name of individual school/ college/ hospital/ unit of the societies/ clubs/ associations.
   - Entity document issued in the name of school/ college/ hospital/ unit of the society. If the entity is a pre-primary or nursery school, which need not be affiliated to any Board as per the law in force in the state concerned, the entity proof need not be insisted upon. In such cases the account would be opened as a unit of the parent entity. (School – Unit of Society/ Trust)
   - Relationship proof between the society and school/ college/ hospital/ unit of the society
   - Site verification Report (SVR) for the school/ college/ hospital/ unit of the society by the Company Official.

d) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents
e) All the KYC documents to be certified under full signature and stamp.

4.4.9. Unincorporated association or a body of individuals: -

One certified copy of each of the following documents or the equivalent e-documents thereof is required to be submitted.

Proof of Existence

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) Documents relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and Documents, as specified in paragraph 4.4.1,
e) Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

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) PAN intimation letter
c) Property or Municipal Tax receipt
d) One-month account statement from existing bank account maintained with a scheduled commercial bank having at least one customer-initiated transaction and not more than 4 months old.
e) Passbook of Scheduled Commercial Bank
f) Rent agreement/ Sale deed with site verification report
g) Registration certificate issued by Central government, State governments, local bodies or statutory authorities having address

Note:

a) Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.
b) Term 'body of individuals' includes societies.
c) The Company shall identify and obtain proof of identity & address of Beneficial owners. 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.

Note: Where the Company is unable to identify the natural person, the identity of the relevant natural person who holds the position of a senior managing official to be recorded with proof of identity and address.

d) A declaration to be obtained that the entity does not accept any Foreign Contribution. No account to be opened if the entity accepts Foreign Contribution.

e) In case the document submitted as proof of existence contains both proof of existence and proof of registered and mailing address, no separate proof of address is required to be furnished.

f) The original of all documents should be sighted by the Company official and the notation "Original Seen and Verified" under his/ her signature and authorised officer code to be mentioned on the copy of KYC documents

g) All the KYC documents to be certified under full signature and stamp.

4.4.10 Judicial Persons

For opening accounts of juridical persons, not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents 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) Officially Valid Documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf

c) Such documents as may be required by the Company to establish the legal existence and address of such an entity/juridical person. In case customer fails to furnish address proof, the Company may accept SVR conducted for verification of address by the Company Official.

d) PAN card/ Form 60, wherever applicable

4.5 Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified as mentioned in paragraph 3(iv) and paragraph of 4.4.1 and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken, keeping in view the following:

a) Where the customer or the owner of the controlling interest is

- an entity listed on a stock exchange in India, or
- it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
- 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 companies.

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

4.6 Transaction Monitoring

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

4.6.2 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.
c) High account turnover inconsistent with the size of the balance maintained.

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

4.6.3 The extent of monitoring shall be aligned with the risk category of the customer.

a) 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.
b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

4.6.4 The Company shall review the transactions flagged as suspicious on a regular basis. Branches shall report the suspicious transactions identified by them to the AML team.

4.6.5 The Board of Directors of the Company shall ensure that an effective AML/CFT program is in place. The AML cell shall exercise continuous monitoring of transactions of all customer accounts. Any suspicious transaction, including attempted transactions, shall be brought into the immediate notice of the Principal Officer. It shall be the duty of the Principal Officer to ensure that a robust reporting system is in place for generating and submitting such suspicious transaction reports.

4.7 Money Laundering and Terrorist Financing Risk Assessment:

a) RE 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.

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, REs shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with RE from time to time.

b) The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the RE to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually

c) The outcome of the exercise shall be placed before the Risk Management Committee of the Board.

d) REs shall apply a Risk Based Approach (RBA) and implement a CDD programme, having regard to the ML/TF risks identified (by the RE itself or through the National Risk Assessment) and the size of business, for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, REs shall monitor the implementation of the controls and enhance them if necessary.

4.8 Compliance of KYC policy

a) The Board of Directors of the RE shall ensure that an effective KYC policy and procedure is in place. In addition, the RE may ensure the following for effective implementation of KYC policy requirements: -

   i. Allocation of responsibility for effective implementation of policies and procedures.

   ii. Independent evaluation of the compliance functions of REs' policies and procedures, including legal and regulatory requirements.

   iii. Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.

   iv. Submission of quarterly audit notes and compliance to the Audit Committee.

b) RE shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

5. Record Management

I. The following steps shall be taken regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. RE shall: -

a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;

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) 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;

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

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

6. Reporting Requirements to Financial Intelligence Unit – India

REs shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. Below are details few returns to be furnished along with due dates: -

Report	Description	Due Date
Cash Transaction Report (CTR)	All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.	15th day of the succeeding month
	All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month	
Suspicious Transaction Report (STR)*	All suspicious transactions whether or not made in cash.	Not later than seven working days on being satisfied that the transaction is suspicious.
Non-Profit Organisation Transaction Reports (NTRs)	Transactions involving receipts by Non-Profit Organisations of value more than Rs. 10 Lakhs or its equivalent in foreign currency	15th day of the succeeding month

*The Company shall adhere to the following instructions while submitting a STR:

i. The definition of suspicious transaction for this policy shall be guided by the definition of suspicious transaction as contained in the PML Act as amended from time to time.
ii. In case the Customer aborts a transaction on being asked to provide more information, it shall be the duty of the Company to report all such attempted transactions (of any amount) in STRs, even if not completed by the customers.
iii. It shall be the duty of the Company to make available a Suspicious Transaction Report in case it has sufficient evidence to believe that a transaction involves criminal proceeds irrespective of the amount of transaction and/or the threshold limit as mentioned in part B of Schedule of PMLA, 2002.
iv. The Company shall furnish a STR within 7 working days of arriving at a conclusion that a transaction, cash or non-cash, or a series of

transactions integrally connected with each other is of suspicious nature. The reason for the same shall be given by the Principal Officer. The Company shall make available such reports to competent authority on request.

v. The Company shall not put any kind of restriction whatsoever on the operations of the account where an STR has been filed. Reporting of STR shall be kept strictly confidential by the Company and its employees as stated under the PML Act.

vi. An essential element to the success of the AML process is that the customers should not be informed (i.e., tipped off) that their accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the designated authority namely Financial Intelligence Unit, India (FIU-IND).

Every RE, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under paragraph 4 (e) of this policy of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

7. Requirements/obligations under International Agreements - Communications from International Agencies

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

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

i. The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", 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/nz8nzen-all.html

ii. 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/nz8nzen-all.html

REs 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 aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council

Resolutions) Order, 2007, as amended from time to time, 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 REs 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 February 2, 2021
In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

c. **Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967: -** The procedure laid down in the UAPA Order dated February 2, 2021 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

a. REs shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India
b. In accordance with paragraph 3 of the aforementioned Order, REs shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
c. Further, REs 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, REs 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. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. REs shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.
e. REs 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, REs shall prevent such individual/entity

from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

g. In case an order to freeze assets under Section 12A is received by the REs from the CNO, REs 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 RE along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

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

D. In addition to the above, REs shall take into account – (a) other UNSCRs and (b) 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.

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

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

a. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be considered. REs shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

b. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The processes referred to in (i) & (ii) above do not preclude RE from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

c. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all

documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

8. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

b) In terms of provision of Rule 9(1A) of PML Rules, the REs shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

d) RE shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

e) The RE other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

f) RE shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

g) Once KYC Identifier is generated by CKYCR, REs shall ensure that the same is communicated to the individual/LE as the case may be.

h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, REs shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in paragraph 4.3.2 of this policy, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the RE obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the RE shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of an existing customer, the RE shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the RE.

i) REs shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

j) For the purpose of establishing an account-based relationship, updation/periodic updation or for verification of identity of a customer, the RE shall seek the KYC

Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

i. there is a change in the information of the customer as existing in the records of CKYCR; or
ii. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
iii. the validity period of downloaded documents has lapsed; or
iv. the RE considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

9. General

9.1 Secrecy Obligations and Sharing of Information:

a) RE shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the RE and customer.
b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
c) While considering the requests for data/information from Government and other agencies, REs 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.
d) The exceptions to the said rule shall be as under:
    i. Where disclosure is under compulsion of law
    ii. Where there is a duty to the public to disclose,
    iii. the interest of REs requires disclosure and
    iv. Where the disclosure is made with the express or implied consent of the customer.
e) Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

9.2 Unique Customer Identification Code (UCIC)

a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by REs.
b) The REs shall, at their option, not issue UCIC to all walk in/occasional customers such as buyers of pre-paid instruments/purchasers of third-party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

9.3 Introduction of New Technologies

REs 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.

Further, REs shall ensure:

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

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

9.4 Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof 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 or equivalent e-document thereof.

9.5 Selling Third party products

RE acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 13(e) of this Directions.
b) transaction details of sale of third-party products and related records shall be maintained as prescribed in Chapter VII paragraph 46.
c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
d) transactions involving rupees fifty thousand and above shall be undertaken only by:
    - debit to customers' account or against cheques; and
    - obtaining and verifying the PAN given by the account-based as well as walk-in customers.
e) Instruction at 'd' above shall also apply to sale of RE own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

9.6 Issuance of Prepaid Payment Instruments (PPIs):

PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

9.7 Hiring of Employees and Employee training

a) Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

b) REs shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff 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 KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

9.8 Appointment of Principal Officer

The Company shall appoint a senior management officer as the Principal Officer (PO). The Principal Officer shall ensure compliance in accordance with the relevant regulatory guidelines, monitor transactions and share and report information as required by the law. The Principal Officer shall act independently and directly report to the senior management or the board of directors.

The Principal Officer shall be responsible for ensuring compliance with the obligations under the PML Act, 2002 amended from time to time.

The name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI & FIU-IND.

9.9 Appointment of Designated Director

The Company shall appoint the Managing Director or Whole Time Director as the Designated Director. The Designated Director shall ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

The name, designation, address and contact details of the Designated Director shall also be communicated to the RBI & FIU-IND.

10. Policy Reviews

The Board shall review and amend this policy as and when required.

If at any point a conflict of interpretation / information between this policy and any regulations, rules, guidelines, notification, clarifications, circulars, master circulars/ directions issued by relevant authorities ("Regulatory Provisions") arises, then interpretation of the Regulatory Provisions shall prevail.

In case of any amendment(s) and/or clarification(s) to the Regulatory Provisions, this policy shall stand amended accordingly from the effective date specified as per the Regulatory Provisions.

Annexure A: Digital KYC Process

A. The RE shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the RE.
B. The access of the Application shall be controlled by the RE 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 RE to its authorized officials.
C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
D. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
E. The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
H. Thereafter, all the entries in the CAF shall 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 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 officer registered with the RE shall not be used for customer signature. The RE 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 RE. 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 RE, 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 RE 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 RE who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Annexure B: Video Based Customer Identification Process (V-CIP)

V-CIP Procedure

A. RE shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the RE 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. Disruption of any sort including pausing of video, reconnecting calls, etc., 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.
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 work flow.
F. The authorised official of the RE 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, in accordance with paragraph 8, using the KYC identifier provided by the customer
    iv. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

    RE shall ensure to redact or blackout the Aadhaar number in terms of paragraph 4.4.1.

    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 working days for usage of Aadhaar XML file / Aadhaar QR code, RE shall ensure that the video process of the V-CIP is undertaken within three 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, RE shall ensure that no incremental risk is added due to this.
G. 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.
H. RE 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 is not valid for the V-CIP.

J. The authorised official of the RE 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. 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.

L. 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.

M. 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 RE.

V-CIP Infrastructure

A. The RE should have complied with 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 RE 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 and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

B. The RE 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 consent should be recorded in an auditable and alteration proof manner.

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

D. 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.

E. 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 RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

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

G. 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.

H. 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.

V-CIP Records and Data Management

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

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

Annexure C: Risk Categorization of Customers

A. Risk Categorisation for Accounts in The Name of Individuals: Risk categorisation for accounts the name of individuals to be done based on type of individual: -

Type	**Recommended Risk Categorization**	**Risk Perception**
Salaried	Low Risk	Source of income is fixed and pattern of entries in the account can be correlated with known sources of income/ expenditure.
Self Employed/ Professionals/ Businessmen	Low Risk (except professionals associated with the film industry who shall be categorized as medium risk)	Accounts maintained by Chartered Accountants, Architects, Lawyers, Doctors, small businesses etc.

Type	Recommended Risk Categorization	Risk Perception
Non-Face to Face Customers	High Risk	Transactions in these accounts to be monitored on concurrent basis.
Non - Resident Individuals	Low Risk	These are highly regulated accounts. All NRI accounts, where the customer has been met face to face and is from a non-high-risk country, shall be categorized as low risk
Politically Exposed Persons	High Risk	Branches should gather sufficient information on any person/ customer of this category intending to establish a relationship and check all the information available on the person in Public Domain. Branches should verify the identity of the persons and seek information about the source of funds before accepting a PEP as customer. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members, close relatives of PEPs and all such accounts where the PEP is an ultimate beneficial owner. The accounts of PEPs resident outside India shall be opened only after obtaining approval of the Senior Management. Further, in the case where an existing customer/ beneficial owner, subsequently becomes PEP - such accounts would be subjected to CDD measures as applicable to the PEP category, including enhanced monitoring on an ongoing basis.
Other Individuals	Low Risk	Residual category as all individual are onboarded after following proper CDD procedure

Note:

a) Any account opened by an individual, as mentioned above, shall be categorized in accordance with the rating mentioned in the Policy.
b) Risk categorisation of customers for whom the Company has filed a Suspicious Transaction Report shall be elevated to High Risk.

B. Risk categorisation for accounts in the name of non-individuals: Risk categorisation for accounts the name of non-individuals to be done based on type of entity & industry: -

TYPE OF ENTITY

Type	**Recommended Risk Categorization**	**Risk Perception**
Private Ltd/ Public Ltd Companies	Low Risk	Governed and registered under Companies Act 1956 / Companies Act 2013
Local Authorities or Local Bodies	Low Risk	Constituted under special acts. Operations are governed under such Acts/ Rules
Public Sector Undertakings, Government Departments/ Undertakings, Statutory Corporations	Low Risk	Governed by specific acts, notifications, etc. framed by the GOI or the state govt. and are controlled and run by the Govt.
Partnership Firm	Low Risk	Registered firms shall be classified as Low Risk. However, unregistered firms shall be categorized as medium risk. Moreover, a partnership firm having a sleeping partner shall be categorized as High Risk
Proprietorship Firm	Medium Risk	These are largely unregistered bodies, and no regulatory/ internal guidelines govern such firms. The Company needs to confirm the existence of the firm and whether the person opening the account is the proprietor of the firm
Trusts – Public Trusts	High Risk	Public Trusts receiving donations pose a higher Money Laundering risk to the Company and therefore proper due diligence is required. All other public trusts are to be classified as Medium Risk

Type	Recommended Risk Categorization	Risk Perception
HUF	High Risk	Unregistered bodies and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Societies/ Associations/ Clubs	High Risk (Except 'Housing Societies' which shall be classified as Low Risk)	These are not highly regulated entities and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Trusts – Private Trusts	High Risk	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known source of income/ expenditure.
Limited Liability Partnerships	Low Risk	Governed and registered under Limited Liability Partnership Act, 2008

Annexure D: Risk Categorisation on the basis of Industry

Risk Category	Industry
High	• Anti-Social organizations and elements. • Politicians and persons with political influence • Lawyers / Advocate / Policeman • Security Services Companies and their Employees, Manpower/Staffing service, Daily wage laborers / Workers • Real estate agents / Builders and their relatives Chit fund companies/Stock Broking/Investment companies and related employees. • Time share companies and related persons, Film producing company • Poultry Farm • Warehouse receipts funding, Merchant exporters, diamond dealer, Bullion trader, • Production or trade in weapons and ammunitions, alcoholic beverages (excluding beer and wine), tobacco • Gambling, casinos and equivalent enterprises. • Production or trade in radioactive materials. This does not apply to the purchase of medical equipment, quality control (measurement) equipment and any equipment where IFC

Risk Category	Industry
	considers the radioactive source to be trivial and/or adequately shielded. • Production or trade in unbonded asbestos fibres. This does not apply to purchase and use of bonded asbestos cement sheeting where the asbestos content is less than 20%. • Drift net fishing in the marine environment using nets in excess of 2.5 km. in length. • Consultant related profiles, Commission agent except agri commission agent • Non-Veg restaurant, Bar • SPA & Gym, Fitness centre • Money lenders/ Private financers • Multi-level marketing (MLM) • Mining work • Entertainment & Art related business, movie halls, malls • Temporary/moveable set-up which is not authorised • Poultry Farm, Butchers • Co-operatives society • Small time Actors, Print & News Media, Press reporters, News reporters, Editors, Journalists. • Collection agencies, Recovery agencies, Verification agencies and their employees, DSAs and their employees • NGO's and their employees • Civil contractors and Labour contractors involved in construction work • Roadside vendors except Food / Snacks Counter and Tea Stalls (no fixed establishment) • Vendors of ABC Pvt. Ltd. • Any contractor engaged into real estate development or related activities viz, colour, electrical, labour, etc • Gems and precious stones business
Medium Risk	• Non-Company Financial Institution • Stock Brokerage • Import/Export (Manufacturers) • Gas Station • Car/Boat/Plane Dealership • Travel Agency • Used car sales • Tele-marketers • Providers of telecommunication service, internet cafes, IDD call service, phone cards, phone centre • Dot-com company or internet business • Pawnshops

Risk Category	Industry	
		• Auctioneers • Notaries (small, little known) • Venture Capital Companies
Low Risk	•	Government departments and Government owned companies, regulatory and statutory bodies
	•	NPOs/NGOs promoted by United Nations or its agencies
	•	Customers with long term and active business relationship with the Company (Not falling under medium or high risk) Any other business not covered above.