Policy on KYC & AML

Version 5.0

"The Company's principals to establish account-based relationship or otherwise with Customers and monitor the transactions."

Contents

Version Control

Document Version	Description of Changes	Date	Prepared / Changed by
1.0	First Version	November 2022	Compliance and Secretarial Department
2.0	Second Version	June 2023	Compliance and Secretarial Department
3.0	Third Version	October 2023	Compliance and Secretarial Department
4.0	Fourth Version	February 2024	Compliance and Secretarial Department
5.0	Fifth Version	March 2025	Compliance and Secretarial Department

A. Background

Ecofy Finance Private Limited (formerly known as Accretive Cleantech Finance Private Limited) (hereafter referred to 'the Company/Ecofy') is a private limited company incorporated under the provisions of the Companies Act, 2013 and is a Non-Banking Finance Company registered with Reserve Bank of India (RBI).

In terms of the provisions of Prevention of Money Laundering Act, (PMLA) 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines applicable to all Non- Banking Financial Companies (NBFCs) as amended from time to time. In view of the same, the Board of Directors of the Company has adopted this policy framework on Anti-Money Laundering (AML), Countering Financing of Terrorism (CFT) and KYC measures in line with RBI guidelines. The Company has formulated this KYC Policy based on RBI's Master Direction- Know Your Customer (KYC) Direction, 2016, dated 25th February 2016, updated from time to time. The Policy is applicable to Ecofy Finance Private Limited (formerly known as Accretive Cleantech Finance Private Limited) and its subsidiary(s).

1. Objectives

1.1. To prevent money laundering or terrorist financing activities;
1.2. To enable the Company to know and understand its customers and their financial dealings better which in turn help the Company to manage its risks prudently;
1.3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
1.4. To comply with applicable laws and regulatory guidelines;
1.5. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

2. Definitions

2.1. "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.
2.2. "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).
2.3. "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.
2.4. "Beneficial Owner" refers to the natural person(s) who ultimately owns or controls a customer and/ or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
2.5. "Updation/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.
2.6. "Certified Copy" - Obtaining a certified copy 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.

2.7. "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.

2.8. "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.

2.9. "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.

2.10. "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.

2.11. "Digital KYC" *means the capturing live photo of the customer* and any one Officially Valid Document ("OVD" where offline verification cannot be carried out, by an authorised officer of the Company).

2.12. "Equivalent e-document" means an electronic equivalent document, issued by the issuing authority 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.

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

1. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
2. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -
    a. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
    b. property or Municipal tax receipt;

c. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
d. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

3. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at '2' above
4. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address

2.14. "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

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

2.16. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company.

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

2.18. "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 Customer Identification Process for the purpose of this Policy.

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

2.20. 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.

3. KYC Process

3.1. Customer Acceptance Policy ("CAP") as set down under Annexure 1. Customer Acceptance Policy shall treat all clients at par without even discriminating especially those, who are financially or socially disadvantaged.

3.2. Customer Identification Procedures ("CIP") as set down under Annexure 2.

3.3. Customer Due Diligence (CDD) Procedures: The features to be verified and documentary proof required from customers of each type and/or their Power of Attorney (POA) holder and/or their Beneficial Owners as set down under Annexure 3 and 4.

3.4. Risk Management - The Company shall have a risk-based approach as set down under Annexure 5. Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception. Risk categorisation shall be broadly undertaken on the basis of parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location, mode of sourcing, nature of underlying loan etc. 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.

4. Responsibility

4.1. The Company shall have a Designated Director appointed by its Board of Directors for the purpose of ensuring overall compliance by the Company under PMLA Act and its Rules. The Company will communicate the name, designation and address of the Designated Director to the FIU-IND and RBI. The Designated Director of the Company shall be the person other than Principal Officer of the Company.

4.2. The Company shall appoint the 'Principal Officer', who will be responsible for ensuring compliance under AML and KYC requirements under PMLA and rules framed thereunder, RBI requirements, CKYC/e-KYC and under such other requirements, monitoring transactions and sharing and reporting information as required under applicable law. The Company will communicate the name, designation and address of the Principal Officer to the FIU-IN and RBI. Principal Officer means an officer at the management level nominated by the Company.

4.3. The Company shall ensure compliance with its KYC policy through –

1. MD, WTD, CRO and Head – Compliance ("Senior Management") to oversee KYC compliance for its effective implementation.
2. Required internal audit and wherever required through concurrent audit to verify the compliance with KYC/AML policies and procedures.
3. Submission of periodical audit reports of the auditors to its Audit Committee.

5. On-going due diligence & evaluation

5.1. The Company would carry out on-going due diligence with respect to the business relationship with every customer closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile, the source of funds/wealth and, wherever necessary, the source of funds. However, the overarching principle for ODD is that the extent of ODD/monitoring would be aligned with the risk category of the customer.

5.2. The Company shall adopt 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. Full KYC exercise shall be carried out, at least once in every two years for high-risk customers, at least once in every eight years for medium risk customers and at least once in every ten years for low-risk customers, from the date of opening of account/last KYC updation.

1. **Individual Customers:**
   a) No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer shall be obtained through customer's email-

id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking), letter etc.

b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of The Company), letter etc., and the declared address shall be verified by the Company at their option. Further, the Company, at their option, may obtain a copy of OVD as defined in clause 2.13 of this Policy 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.

c) 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.

2. Non-individual Customers:

a) No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration shall be obtained from the LE customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking), letter from an official authorized by the LE in this regard, board resolution etc. Further, the 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

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

3. **Additional measures:** In addition to the above, the Company shall ensure that –

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

b) 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.

c) The Company shall ensure to provide acknowledgment to the customer with date of having performed KYC updation/periodic updation.

d) The Company shall adopt a risk-based approach with respect to periodic updation of KYC

4. The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of

establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Company' end.

5. In case of existing customers, the Company shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60 of the customer. Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, the Company shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring. Provided further that if a customer having an existing account-based relationship with the Company gives in writing to the Company that he does not want to submit his Permanent Account Number or equivalent e- document thereof or Form No.60, the Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

5.3. 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. Higher risk accounts shall be subjected to intensify monitoring.

5.4. As a risk-mitigating measure for such accounts, the Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. In case of request of change of mobile number from the customer, below steps to be followed:

5.4.1. The customer to initiate forma request from registered email id or letter to the Company for change of mobile number, (the mobile number should be linked with Aadhaar),

5.4.2. On receipt of formal request from the Customer, RE to initiate Aadhaar based otp verification of mobile number,

5.4.3. Post successful verification of mobile number, the customers' details to be updated in the records of the Company.

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

6. Enhanced due-diligence

6.1. Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):

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

a) In case the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. The Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

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

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

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

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

Accounts of Politically Exposed Persons (PEPs).

The Company shall have the option of establishing a relationship with PEPs provided that:

The Company 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:

a) The Company has in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
b) Reasonable measures are taken by the Company for establishing the source of funds / wealth;
c) the approval to open an account for a PEP shall be obtained from the senior management level in accordance with the Company's Customer Acceptance Policy
d) all such accounts are subjected to enhanced monitoring on an on-going basis
e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship
f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable

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

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

7. Record Management

7.1. All transaction records including KYC documents obtained from customers under the policy would be maintained for a period of Five (5) years from the date of transaction.

7.2. 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;

7.3. Make available swiftly the identification records and transaction data to the competent authorities upon request;

7.4. Maintain records of the identity and address of their customer, and records in respect of transactions.

7.5. Records should contain all the information necessary to permit the reconstruction of the individual transaction including the following information:

1. Nature of the transactions,
2. Amount of the transaction and the currency in which it was denominated,
3. The date on which the transaction was conducted,
4. Parties to the transaction

7.6. As required under RBI regulations, the Company shall ensure filing of all required Suspicious Transaction Report (STR) and Cash Transaction Report (CTR) to Financial Intelligence Unit (fiu) – India within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

7.7. The Principal Officer should record his reasons for treating any transaction as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or other office. Such report shall be made available to the competent authorities on request. Illustrative list of activities which would be construed as suspicious transactions is given in Annexure 6. Any changes required due to business exigencies or due to regulatory / audit requirements, will be required to be approved by Principal Officer, appointed under this Policy.

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

8. Monitoring

8.1. On-going monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. The Company must pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The extent of monitoring shall be aligned with the risk category of the customer. Higher risk accounts shall be subjected to intense monitoring.

8.2. The following activities may form part of the monitoring function:

1. The account of the Customer after signing of the contract to be closely monitored for signs of any unusual transactions;
2. All Cash & suspicious transactions are required to be reported within the timelines

given under Prevention of Money laundering Act ('PMLA'), 2002; the PML Rules 2005 framed thereunder; and the Foreign Regulation Act 2010

3. High-risk accounts shall be subjected to intensified monitoring;
4. The Company should maintain a record of all transactions and take steps to preserve the same.

9. Reporting Transactions

9.1. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) shall be adhere to as per provisions of Income Tax Rules.

9.2. The Company should not put any restriction on operations in the accounts where an STR has been made. It should also be ensured that there is no tipping off to the customer at any level.

9.3. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious.

9.4. RBI has clarified that FINnet gateway portal has to be used for uploading of STR. FIU has enabled Web filing for uploading STR in both Account based Reporting Format (ARF) and Transaction based Reporting Format (TRF). Web filing involves data entry of details on an online web page for submitting reports to FIU-IND.

9.5. Following reporting are required to FIU by 15th of the succeeding month:

1. All cash transactions of the value of Rs. 10 lakhs and above or its equivalent in foreign currency;
2. All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate is Rs. ten lakh rupees and above or its equivalent in foreign currency.
3. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions
4. All transactions involving receipts by non-profit organizations of value more than Rs.Ten lakhs or, its equivalent in foreign currency
5. All Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

9.6. As required under RBI regulations, the Company shall ensure filing of all required Suspicious Transaction Report (STR) and Cash Transaction Report (CTR) to Financial Intelligence Unit (fiu) – India within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

9.7. The Principal Officer should record his reasons for treating any transaction as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or other office. Such report shall be made available to the competent authorities on request. Illustrative list of activities which would be construed as suspicious transactions is given in Annexure 6.

9.8. Any changes required due to business exigencies or due to regulatory / audit requirements, will be required to be approved by Principal Officer, appointed under this Policy.

10. Internal ML/ TF Risk Assessment

The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

While assessing the ML/TF risk, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time. Further, the internal risk assessment shall be carried in commensurate to its size, geographical presence, complexity of activities/structure, etc.

Also, the Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall have adequate controls and procedures in this regard as per the size of the business. The Implementation of controls to be monitored regularly and enhancement to be done if necessary.

As per the regulatory requirement specified in the circular, such internal risk assessment shall be done periodically but not later than annual and shall be presented to Board/Risk Management Committee.

11. Employee Training

Periodic training programmes will be organized for employees to have adequate screening mechanism as an integral part of their personnel recruitment/hiring process.

On-going employee training programme shall be put in place so that the employees 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 Company, regulation and related issues shall be ensured shall be put in place in AML procedures.

12. Confidentiality

Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer. The exceptions to the said rule shall be as under:

12.1 Where disclosure is under compulsion of law;

12.2 Where there is a duty to the public to disclose;

12.3 The interest of bank requires disclosure and;

12.4 Where the disclosure is made with the express or implied consent of the customer

13. Other Information

13.1. The Company shall pay adequate attention to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied

before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures

13.2. Unique Customer Identification Code ("UCIC") shall be allotted while entering new relationships with the individual customers as also the existing individual customers.

13.3. The Company shall review the policy on an annual basis or at earlier intervals, if there any regulatory changes necessitating such interim reviews.

14. Introduction of New Technologies:

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

14.2. Further, the Company shall ensure:

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

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

15. Requirements/obligations under International Agreements - Communications from International Agencies:

In order to prevent the Company from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

The Company 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 Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The 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 Company for meticulous compliance.

The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India as updated from time to time.

The Company 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.

B. Annexures

1. Annexure 1

Customer Acceptance

1.1 No account shall be opened by The Company in anonymous or fictitious/benami names.

1.2 No account shall be 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.

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

1.4 The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation shall be as specified by the Policy and as amended or specified from time to time. Any exceptions shall be discussed with the Principal Officer.

1.5 Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.

1.6 The 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.

1.7 CDD Procedure is followed for all the joint account holders, while opening a joint account.

1.8 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 circulated by Reserve Bank of India.

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

1.10 Verified that identity of the customer does not match with any person or entity, whose name appears in the sanctions list circulated by Reserve Bank of India.

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

1.12 Where the Company 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.

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

2. Annexure 2

Customer Identification Procedures

Customer identification means identifying the customer and verifying his / her / its identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as PAN, Voter ID card / Passport / Officially Valid Documents, etc. necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Company will not insist on obtaining Aadhar except for those accounts intended to receive government subsidies /subvention or benefits under direct benefit transfer

scheme of the Government. However, customer voluntarily producing Aadhar for the purpose of identification will be accepted by the company.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, Company shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall

2.1 verify the legal status of the legal person/ entity through proper and relevant documents
2.2 verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person.

Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. An indicative list of the nature and type of documents/information that may be relied upon for Customer Identification Procedure as given in **Annexure 4**.

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

2.3 Commencement of an account-based relationship with the customer.
2.4 When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
2.5 As and when applicable, selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.

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

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.

2.6 The Company shall take adequate steps 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.
2.7 The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act
2.8 The third party shall not be based in a country or jurisdiction assessed as high risk.
2.9 The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the Company.

3. Annexure 3

Customer Due Diligence (CDD) Procedure in case of Individuals

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

3.1 the Aadhaar number where,

1. he/she is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
2. he/she decides to submit Aadhaar number voluntarily to the Company notified under first proviso to sub-section (1) of section 11A of the PML Act; or
    a) the proof of possession of Aadhaar number where offline verification can be carried out; or
    b) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

3.2 the KYC Identifier with an explicit consent to download records from CKYCR

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

3.4 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 Company:

Provided that where the customer has submitted,

1. proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.
2. an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Digital KYC Process.
3. any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under Digital KYC Process.
4. KYC Identifier, the Company shall retrieve the KYC records online from the CKYCR in accordance with this Policy.

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

In case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme, owing to injury, illness or infirmity on account of old age or otherwise and similar causes, the Company shall apart from obtaining the Aadhar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit.

The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review.

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

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

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

Note:

1. PAN Card shall be verified electronically from NSDL so as to ascertain correctness of PAN Number and corresponding name appearing in Income Tax data base. The said verification may be carried out by the Company itself or through an independent Agency.
2. Similarly, AADHAR, Driving License & Voters ID shall be verified through Independent Agency.
3. Utility Bills and Passport will be used to verify address
4. Customer will electronically upload his selfie.
5. Bank statement will be used to verify bank account number.

Accounts Opened through OTP based e-KYC - (Master Direction - Know Your Customer (KYC) Direction, 2016)

The company may provide an option for One Time Pin (OTP) based e-KYC process for onboarding of customers. Accounts opened in terms of this provision i.e., using OTP based e-KYC, are subject to the following conditions:

1. There must be a specific consent from the customer for authentication through OTP.
2. Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
3. Account, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per this policy. If Aadhaar details are used, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
4. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non face-to-face mode with any other Regulated Entity (RE). Further, while uploading KYC information to CKYCR, the company shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

4. Annexure 4

Customer Identification Procedure

Certified documents or its equivalent e-documents that shall be obtained from the customers at the time of account opening are as below:

Customers	Documents
Individuals and individual (sole proprietor) proof of identity and proof of residence	One of the following certified Document or the lent e-documents thereof viz., 1. Passport
	2. Aadhaar Card (mandatory for any subsidy benefit) or Proof of possession of Aadhaar issued by UIDAI or E-Aadhaar.
	3. Voter's Identity Card issued by the Election Commission of India
	4. Driving License
	5. Job card issued by NREGA duly signed by an officer of the State Govt.
	Letter issued by Registrar of National Population Register containing details of name and address And Permanent Account Number (PAN) or Form No. 60 as per Income Tax Rules 1962. (Mandatory along with one of the OVDs) Provided that, where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. 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 Gazette notification or marriage certificate issued by the State Government, indicating such a change of name. 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:
	(i) Utility bill (electricity, telephone, post-paid mobile phone, piped gas, water bill) not more than 2 months old (ii) Property or municipal tax receipt; (iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (iv) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation; In case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address Provided further that the customer shall submit updated OVD with current address within a period of three months of submitting the above documents.

Sole Proprietorship Firm	Apart from Customer identification procedure as applicable to the proprietor any two of the following certified copy of documents or equivalent e-documents thereof in the name of the proprietary concern would suffice: (i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government. (ii) Certificate/ license issued by the municipal authorities under Shop and Establishment Act. (iii) Sales and income tax returns. (iv) CST/VAT/GST certificate (provisional/ final) (v) Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities. (vi) 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. (vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax authorities.
	(viii) Utility bills such as electricity, water, and landline telephone bills In cases where the Company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as activity proof. In such cases, the Company, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy that the business activity has been verified from the address of the proprietary concern.
Company	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Certificate of incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the company; (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; (v) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (vi) the names of the relevant persons holding senior management position; and (vii) the registered office and the principal place of its business, if it is different

Partnership Firms	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Registration certificate; (ii) Partnership deed; (iii) Permanent Account Number of the partnership firm; (iv) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (v) the names of all the partners and (vi) address of the registered office, and the principal place of its business, if it is different.
Trusts & Foundations	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Certificate of registration, if registered ii. Trust Deed iii. Permanent Account Number or Form No.60 of the trust iv. Power of Attorney granted to transact business on its behalf v. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors Resolution of the managing body of the foundation/association vi. the names of the beneficiaries, trustees, settlor, protector if any, and authors of the trust vii. the address of the registered office of the trust; and viii. list of trustees and documents, as specified for Individuals, for those discharging the role as trustee and authorised to transact on behalf of the trust.
Unincorporated Association or Body of Individuals	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Resolution of the managing body of such association or body of individuals ii. power of attorney granted to him to transact on its behalf iii. PAN or Form 60 of the unincorporated association or body of individuals iv. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the person holding an attorney to transact on its behalf Such other documents as may be required by Company to collectively establish the legal existence of such as association or body of individuals.

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

Beneficial Ownership Guidelines: -

1. Rule 9 (1A) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and

take all reasonable steps to verify his identity.
2. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

Beneficial Owner (BO) means:

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

   Explanation- For the purpose of this sub- clause-

   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.

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

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 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 relevantnatural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

e. For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents 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. Documents, as specified for the Indivduals, of the person holding an attorney to transact on its behalf and

c. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

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

1) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.;
2) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee, or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Further, while undertaking customer identification, the Company shall also be ensured that:

1) Decision-making functions of determining compliance with KYC norms are not outsourced.
2) Introduction is not sought while opening accounts.

Direction for Selling Third party products

If in the future, the Company acts as agent while selling third party products, it shall comply with the applicable laws/regulations, including system capabilities for capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customer.

Video based Customer Identification Process (V-CIP)

The Company may undertake live V-CIP to be carried out by their official for establishment of an account based relationship with a new individual customer, proprietor (in case of proprietorship firm), authorized signatories and Beneficial Owner (BO) (in case of Legal Entity (LE) customers), conversion of existing accounts opened in non-face to face mode and updation/periodic updation of KYC for eligible customers, after obtaining his informed consent and shall adhere to the following stipulations:

1. **V-CIP Infrastructure**

a) The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilienceframework, as well as other general guidelines on IT risks.
b) The Company shall have in-house infrastructure in its own premises and the V-CIP connection and interactionshall originate from its own secured network domain. The Company shall also comply with the Outsourcing Guidelines issued by RBI for any technology related outsourcing activities. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.
c) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

d) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
e) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
f) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with The Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
g) The Company shall regularly upgrade technology infrastructure including application software as well as workflows based on experience of detected / attempted / 'near-miss cases of forged identity. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.
h) The Company shall conduct necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities of V-CIP Infrastructure.Any critical gap reported under this process shall be mitigated before rolling out its implementation. The Company shall engage suitably accredited agencies as prescribed by RBI to conduct such tests periodically in conformance to internal / regulatory guidelines.
i) The Company shall conduct appropriate testing of function, performance and maintenance strength of the V- CIP application software and relevant APIs / webservices etc. before being used in live environment. Only after closure of any critical gap found during such tests, The Company shall roll out the application. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

2. **V-CIP Procedure**

a) The Company shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of The Company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
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 Company. However, in case of call drop / disconnection, fresh session shall be initiated.
c) The official of The Company shall ensure that if there is a disruption in the V-CIP procedure, the same shall be aborted and a fresh session shall be initiated.
d) 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
e) Any prompting, observed at end of customer shall lead to rejection of the account opening process
f) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.
g) The authorised official of The Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification informationusing any one of the following:

1) OTP based Aadhaar e-KYC authentication

2) Offline Verification of Aadhaar for identification
3) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer
4) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi-locker

The Company shall ensure to redact or blackout the Aadhaar number.
In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, The Company shall ensure that the XML file or QR code generation date is not older than 3 working days from the date of carryingout V-CIP.

Further, in line with the aforesaid prescribed period, The Company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, The Company shall ensure that no incremental risk is added due to this.

a) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured. The Company shall ensure that the economic and financial profile/information submitted by the customer is also confirmed from the customer while undertaking the V-CIP in a suitable manner.
b) The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi locker.
c) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
d) The authorised official of The Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP, and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
e) 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.
f) The Company shall comply with all such matters required under other statutes, such as the Information Technology (IT) Act.

3. **V-CIP Records and Data Management**
   a) The Company shall store the entire data and recordings in a system(s) located in India, in a safe and secured manner and shall bear time and date stamp for easy historical search.
   b) The Company shall follow the provisions of Record Management as contained in this Policy.
   c) The activity log along with credential of the official performing V-CIP shall be preserved.

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

a) The Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
b) Operational Guidelines for uploading the KYC data have been released by CERSAI.

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

d) The Company were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, and KYC records pertaining to accounts of Legal entities opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid.

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

f) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, The Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates at the time of periodic updation, 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 (h) below 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.

g) The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

h) Where a customer, for the purposes 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

    1) there is a change in the information of the customeras existing in the records of CKYCR;
    2) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms;
    3) the current address of the customer is required to be verified;
    4) the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
    5) The validity period of documents downloaded from CKYCR has lapsed.

5. Annexure 5

Risk Management

Risk Categorization: Indicative guidelines

As per the KYC policy, for acceptance and identification, the Company's Customers would be categorized based on perceived risk, broadly into three categories – A, B & C. Category A would include High Risk Customers, Category B would include Medium Risk Customers while Category C would include Low Risk Customers.

None of the Customers will be exempted from the Company's KYC procedures, irrespective of the status and relationship with Company or its Promoters. The due diligence to be exercised would depend on the risk categorisation of the customers. Enhanced due diligence will be carried out in respect of customers falling in the medium and high-risk category.

The Company currently lends to salaried Indian resident. Board categorization is based on income, age profile, credit bureau and other obligations of the customer. Individuals whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk by the Company. In such cases, the Policy may require that only the basic requirements of verifying the identity and location of the Customer are to be met. Customers that are likely to pose a higher-than-average risk to the Company will be categorized as medium or high risk depending on Customer's background, nature, location of activity, and profile etc. The Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

Customer risk category should include:

5.1 High Risk-High risk customers typically include:

1. Non-resident customers
2. High net worth individuals without an occupation track record of more than 3 years
3. Trust, charitable organizations, Non-Government Organization (NGO), organizations receiving donations;
4. Companies having close family shareholding or beneficial ownership;
5. Firms with sleeping partners;
6. Politically exposed persons (PEPs) of Indian/ foreign origin;
7. Person with dubious reputation as per public information
8. Company name changed in last 2 years
9. Irregular/Delay in compliance – GST, PF, etc. by an entity.
10. Any other risk perceived by Credit during assessment.
11. Customer onboarded via non face to face mode.

5.2 Medium Risk-Medium Risk customer will include:

1. Salaried applicant with variable income/ unstructured income receiving Salary in cheque/cash.
2. Salaried applicant working with, Proprietary, Partnership firms;
3. Self- employed professionals other than HNIs.
4. Self-employed customers with sound business and profitable track record for a reasonable period;
5. High Net worth individuals with occupation track record of more than 3 years;
6. Source of Funds is not clear.
7. Company Profile-Location of company, Low net worth promoters, any negative news which is more than 5 years old.
8. Any other risk perceived by Credit during assessment.

5.3 Low Risk-Low Risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified, and all other person not covered under above two categories. Customer carrying low risk may include the following:

1. Individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified, and all other persons not covered under above two categories.
2. Salaried employees with well-defined salary structures;
3. People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies etc.
4. If the profile is assessed to be low risk by credit due to strong mitigations available.

Important for Risk categorization:
If the client falls under more than one Risk category, then higher Risk Category shall apply. E.g., If the client is in the Low-Risk category and also a PEP (i.e., High Risk category), then the Client would be considered in the High-Risk category.

6. Annexure 6

Illustrative list of activities which would be construed as suspicious transactions

6.1 Activities not consistent with the customer's business, i.e., accounts with large volume of creditswhereas the nature of business does not justify such credits.

6.2 Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:

1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
2. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
3. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

6.3 Certain Employees of the Company arousing suspicion:

1. An employee whose lavish lifestyle cannot be supported by his or her salary.
2. Negligence of employees/wilful blindness is reported repeatedly.

6.4 The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

6.5 Some examples of suspicious activities/transactions to be monitored by the operating staff:

1. Multiple accounts under the same name
2. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc;
3. There are reasonable doubts over the real beneficiary of the loan
4. Frequent requests for change of address.