KYC, AML & CFT POLICY

Standard Capital Markets Limited

Table of Contents

DOCUMENT IDENTIFICATION INFORMATION

Document Name	KYC, AML & CFT Policy
Index	Corporate Governance/ Know Your Customer & Anti-Money Laundering Policy and Procedures
No. of Pages	48
Approving Authority	Board of Directors
Review Frequency	Reviewed if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

This policy is issued by STANDARD CAPITAL MARKETS LIMITED (hereinafter referred to as "SCML" or "Company") and encompasses all affiliated entities, employees, and stakeholders associated with SCML's operations.

1. Policy Statement

1.1. SCML is committed to implementing robust and comprehensive measures for Know Your Customer (KYC), Anti-Money Laundering (AML), and Combating Financing of Terrorism (CFT) in line with regulatory requirements.

1.2. This policy has been formulated in strict compliance with the *Reserve Bank of India's Master Direction – Know Your Customer (KYC) Direction, 2016, the Prevention of Money Laundering Act, 2002 (PMLA*), and other applicable laws and guidelines.

1.3. The policy is designed to establish a framework for customer identification, due diligence, and risk management to prevent the misuse of financial systems for money laundering, terrorist financing, and other illicit activities.

1.4. The company shall adopt a risk-based approach to ensure effective compliance, safeguarding the integrity of its operations. All employees of SCML are expected to uphold this policy and maintain the highest standards of ethical conduct in dealing with customers.

2. Definition & Interpretation

In this policy, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

2.1. "Aadhaar Number" refers to the unique identification number issued to an individual under section 3(3) of *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016.*

2.2. "Authentication" refers to the process by which an individual's Aadhaar number, along with their demographic or biometric information, is submitted to the Central Identities Data Repository (CIDR) for verification. The Repository authenticates the correctness or otherwise of the submitted information based on the data available within it, as outlined under *The Aadhaar Act, 2016.*

2.3. "Central KYC Records Registry" refers to an entity as defined under *Rule 2(1) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.* It is established to receive, store, safeguard, and retrieve the KYC records of customers in a digital form for use by reporting entities, ensuring uniformity and efficiency in KYC compliance across the financial sector.

2.4. "Designated Director" refers to a person appointed by the Company to ensure overall compliance with the obligations

under *Chapter IV of the Prevention of Money Laundering Act, 2002 (PMLA) and the associated rules.*

2.5. "Digital KYC" refers to the process of capturing a live photograph of the customer along with their officially valid document or proof of possession of Aadhaar, where offline verification is not possible. This process also includes capturing the latitude and longitude of the location where the live photo is taken.

2.6. "Digital Signature" means the authentication of any electronic record by a subscriber using an electronic method or procedure in accordance with the provisions of *Section 3 of the Information Technology Act, 2000.*

2.7. "Equivalent E-Document" means an electronic version of a document issued by the issuing authority with a valid digital signature, including documents issued to a customer's digital locker account.

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

2.9. "Officially Valid Document" refers to any document recognized as valid for the purpose of customer identification under the PMLA, 2002 and related regulations. Specifically, it includes documents such as a passport, voter ID, driving license, Aadhaar card, or any other government-issued identification document, as defined by the RBI and relevant regulatory authorities.

2.10. "Offline Verification", as defined in the *Aadhaar and Other Law (Amendment) Ordinance, 2019*, means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

2.11. "Person" includes any individual, Hindu Undivided Family (HUF), company, firm, association of persons, body of individuals (incorporated or not), artificial juridical person, and any agency, office, or branch owned or controlled by the above entities.

2.12. "Principal Officer" means an officer at the management level, nominated by the company for ensuring company's compliance with legal obligations related to KYC, AML, and other regulatory requirements.

2.13. Suspicious Transaction" means a transaction, including an attempted transaction, whether or not made in cash, which raises reasonable grounds of suspicion for a person acting in good faith, including proceeds of an offence specified in the Schedule to the PMLA, 2002, irrespective of the value involved.

2.14. "Transaction" refers to any act of purchasing, selling, loaning, pledging, gifting, transferring, or delivering, Deposits, withdrawals, exchanges, or transfers of funds in any currency, whether in cash, cheque, payment order, or by electronic means.

2.15. "Customer" refers to a person who is engaged in a financial transaction or activity with the company.

2.16. "Customer Due Diligence (CDD)" refers to the process of identifying and verifying the customer using reliable and independent sources of identification.

2.17. "Customer identification" means undertaking the process of CDD.

2.18. "Officially Valid Documents" means Passport, driving licence, Aadhaar Card, Voter's Identity Card, Job card issued by NREGA duly signed by an officer of the State Government, or any other officially valid documents issued by the Government Authorities.

2.19. "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.

2.20. "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 RBI.

2.21. "Video-based Customer Identification Process (V-CIP)" is an alternative method for customer identification through a secure, live, informed-consent video interaction. It involves facial recognition and verification of the information provided by the customer for Customer Due Diligence (CDD) purposes, maintaining an audit trail.

2.22. "Politically Exposed Persons" shall refer to Heads of States or Governments, Senior politicians, Senior government, judicial, or military officials, Senior executives of state-owned corporations, and Important political party officials.

2.23. "Money laundering" is defined in Section 3 of the Prevention of Money Laundering Act, 2002 (PMLA) as "whosoever directly or indirectly attempts to indulge or knowingly assists or is knowingly a party to or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of the offence of money laundering.

2.24. "UCIC" means Unique Customer Identification Code.

2.25. "Account" shall be deemed to refer to a "loan account" maintained with the company, unless explicitly specified otherwise. This clarification is in alignment with the operational framework of NBFCs, wherein accounts primarily pertain to credit facilities extended to customers.

3. Objectives of the Policy

3.1. The objective of prescribing KYC/AML/CFT guidelines is to enable SCML to know/understand the customers and their financial dealing better, thereby helping all concerned staff to manage KYC, AML, CFT related risks prudentially.

3.1.1. To implement a proper mechanism for the verification of the customers through KYC.

3.1.2. To prevent misuse of SCML for money laundering or terrorist financing.

3.1.3. To implement controls for detecting and regulating suspicious transactions.

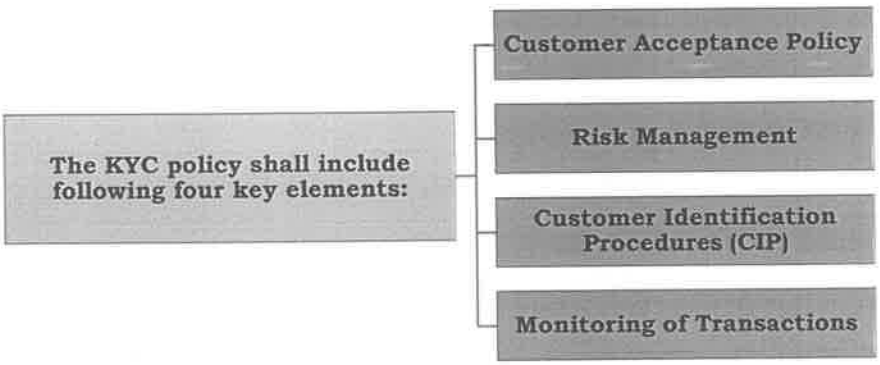
3.1.4. To ensure compliance with PMLA, 2002 and its amendments.

3.1.5. To adhere to guidelines from FIU-IND and RBI.

4. Scope & Applicability of the Policy

4.1. The policy applies to all customers, transactions, and operations of SCML, covering processes related to CDD, ongoing monitoring, and record-keeping.

4.2. The policy is applicable across all branches, offices, and employees of SCML, including agents, to prevent money laundering, terrorism financing, and other illicit activities.



5. Governance Framework for KYC Compliance

5.1. The Designated Director and Principal Officer shall be appointed by the Board to ensure compliance with PMLA 2002 and associated Rules.

5.2. Under no circumstances shall the Principal Officer be nominated as the Designated Director.

5.3. The Principal Officer shall be responsible for:

5.3.1. Ensuring compliance with all the provisions as outlined in this KYC/AML/CFT policy.

5.3.2. Monitoring transactions and sharing and reporting information as required under the law/regulations.

5.4. The Designated Director & Principal Officer's details (Name, Address and Designation) shall be communicated to FIU-IND and RBI.

5.5. Compliance Measures:

5.5.1. Identification of senior management responsible for overseeing KYC/AML compliance.

5.5.2. Allocation of responsibilities for implementing policies.

5.5.3. Independent evaluations and audits to ensure regulatory compliance.

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

5.5.5. Quarterly audit reports submitted to the Audit Committee.

5.6. KYC-related decisions, including customer identification and verification, will not be outsourced.

5.7. Details of the Designated Director and Principal Officer shall be maintained in **Annexure-A** of the Policy for submission to authorities.

6. Customer Acceptance Policy (CAP) & Procedures

6.1. The Customer Acceptance Policy (CAP) of SCML aims to ensure compliance with KYC and AML norms by establishing guidelines for customer onboarding and management while avoiding any form of discrimination, especially against financially or socially disadvantaged members of society.

6.2. No account shall be opened in an anonymous or fictitious/benami name.

6.3. Accounts shall not be opened if the company is unable to perform Customer Due Diligence (CDD) due to:

6.3.1. Non-cooperation from the customer; or

6.3.2. Unreliable or insufficient documents/information provided by the customer.

6.3.3. In such cases, the company may consider filing a Suspicious Transaction Report (STR) with FIU-IND.

6.4. Customers shall furnish mandatory information and documents for KYC purposes during account opening and periodic updates.

6.5. Verification of Permanent Account Number (PAN) shall be conducted using the issuing authority's verification facility.

6.6. The CDD procedure shall be applied at the Unique Customer Identification Code (UCIC) level. For existing KYC-compliant customers, no fresh CDD is required for availing of additional services, provided their identification is already verified.

6.7. Where a customer is acting on behalf of another person or entity, such authorization and circumstances shall be clearly documented.

6.8. A suitable system shall be implemented to ensure that the customer's identity does not match any name listed in sanction lists or other restricted entities as specified in relevant guidelines.

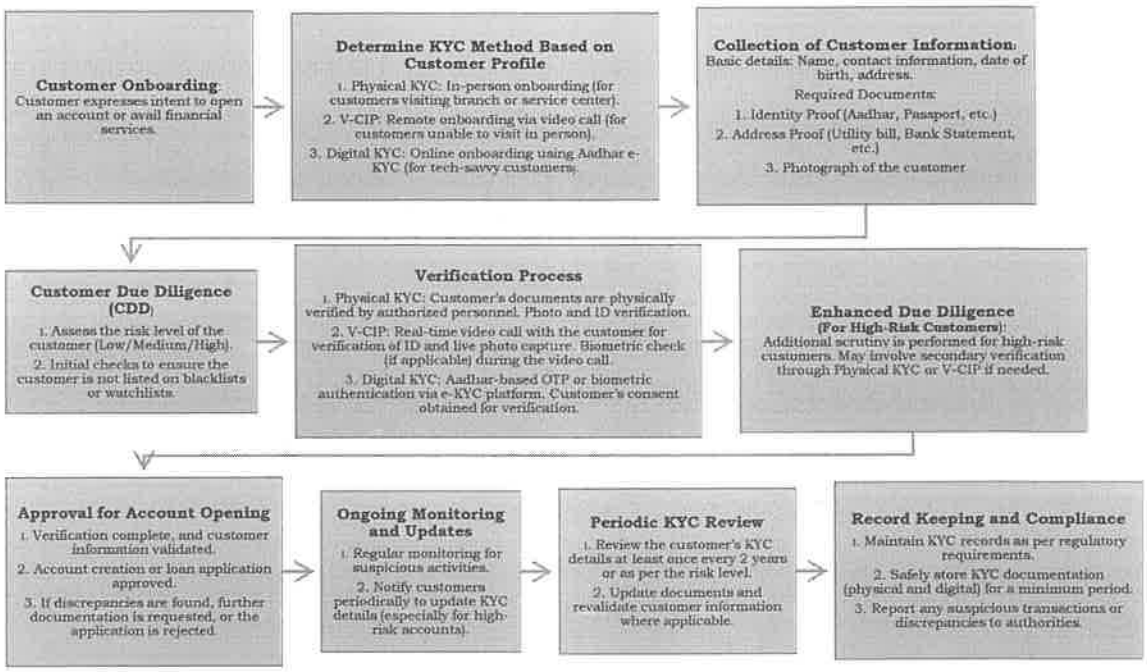
6.9. If equivalent e-documents are submitted by the customer, the digital signature on such documents shall be verified in compliance with the Information Technology Act, 2000.

6.10. If SCML suspects money laundering or terrorist financing and reasonably believes that completing the CDD process would tip off the customer, SCML shall:

6.10.1. Suspend the CDD process; and

6.10.2. File an STR with FIU-IND without notifying the customer.

6.11. SCML shall allocate responsibility for effective implementation of the CAP. The policy and its implementation shall be independently evaluated through audits and internal monitoring systems.



7. Risk Management Framework

7.1. SCML shall adopt a risk-based approach for customer due diligence and ongoing monitoring, ensuring effective management and mitigation of risks associated with money laundering and terrorist financing. The following principles shall govern risk management:

7.1.1. Customers shall be categorized into low, medium, and high-risk categories based on SCML's risk perception and assessment, considering factors such as identity, social/financial status, nature of business, and location.

7.1.2. Risk categorization shall be based on, but not limited to, the following parameters:

7.1.2.1. Customer Identity: Verification of identity documents and their authenticity through issuing authorities' services.

7.1.2.2. Social/Financial Status: Nature and volume of the customer's financial activity.

7.1.2.3. Nature of Business/Occupation: Assessment of the customer's business activity and its inherent risks.

7.1.2.4. Geographical Risk: Assessment of the customer's location and transactions, particularly those involving high-risk jurisdictions.

7.1.2.5. Type and Delivery Channels of Products/Services: The type of Products/Services offered by the Company and the delivery channels used for delivery of such products/services.

7.1.2.6. Type of Transaction: The type of transaction undertaken whether cash, cheque/monetary instruments, wire transfers, forex transactions, etc.

7.1.3. The categorization of a customer and the reasons for their risk classification shall remain strictly confidential and not be disclosed to the customer to prevent tipping off.

7.1.4. SCML shall establish mechanisms for periodic review and reassessment of customer risk categorization based on transaction history, changes in business activity, and regulatory updates.

7.1.5. Information collected for risk assessment purposes shall be non-intrusive and in compliance with the KYC/AML policy.

8. Customer Identification Procedure (CIP)

8.1. SCML shall establish and implement a comprehensive Customer Identification Procedure (CIP) in compliance with applicable regulations under the PMLA, RBI guidelines, and other relevant regulatory provisions.

8.2. SCML shall undertake the CIP process in the following circumstances:

8.2.1. At the commencement of a loan account-based relationship with a customer.

8.2.2. When there is any doubt regarding the authenticity or adequacy of customer identification data previously obtained.

8.2.3. In case of changes in the nature or scope of the business relationship with the customer that warrant re-identification, including cases where the customer's risk profile has changed.

8.3. SCML shall verify the identity of its customers using reliable, independent, and officially valid documents, ensuring compliance with the KYC norms as prescribed by the RBI.

8.4. SCML shall verify and retain the customer's identity details in accordance with applicable laws.

8.5. Customer Due Diligence (CDD) Reliance on Third Parties: SCML may rely on customer due diligence measures performed by a third party, subject to the following conditions:

8.5.1. SCML obtains records or information related to CDD performed by the third party immediately or from the Central KYC Records Registry (CKYCR).

8.5.2. SCML ensures that copies of identification data and other relevant documentation are available from the third party upon request without delay.

8.5.3. The third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements under the PMLA.

8.5.4. The third party is not based in a jurisdiction identified as high-risk by regulatory or international advisories.

8.5.5. SCML evaluates the reliability of the third party's CDD process and verifies the data periodically.

8.6. The information collected during the CIP process shall be non-intrusive and in line with the customer's right to privacy. SCML shall take reasonable measures to protect the confidentiality of the data.

8.7. When third-party reliance is exercised, SCML remains accountable for the accuracy, authenticity, and integrity of customer identification and due diligence processes.

8.8. SCML shall establish and maintain an effective system for ongoing monitoring of customer transactions including identifying and reporting any suspicious transactions, including those that may involve money laundering or financing of terrorism, as per PMLA and RBI regulations.

8.9. SCML shall periodically review and update its CIP in line with evolving regulatory requirements, including any amendments to the PMLA, RBI guidelines, or other relevant laws.

9. CIP: Framework & Implementation

9.1. To comply with the KYC requirements under the Prevention of Money Laundering Act, 2002, and applicable RBI guidelines, SCML shall adopt the following procedures to verify the identity of customers before establishing any account-based relationship or transaction:

9.1.1. **Physical Customer Identification Procedure (CIP):**

9.1.1.1. The customer's identity shall be verified through face-to-face interaction at SCML's branch or authorized location.

9.1.1.2. Original OVDs or equivalent e-documents shall be obtained and verified for identity and address proof.

9.1.1.3. A photograph of the customer, as well as their signature/thumb impression, shall be captured in the presence of SCML's personnel.

9.1.1.4. Copies of OVDs shall be retained, with a remark by SCML staff certifying the authenticity of the verification.

9.2. **Video-Based Customer Identification Procedure (V-CIP):**

9.2.1. SCML shall offer video-based identification to customers as an alternative to physical verification.

9.2.2. The V-CIP process shall be conducted by trained personnel and involve live interaction with the customer.

9.2.3. During the interaction, the customer's photograph, valid OVD, and signature/thumb impression shall be captured using end-to-end encrypted video recording.

9.2.4. Aadhaar authentication (via e-KYC or offline verification) may also be performed during the session if voluntarily provided by the customer.

9.2.5. "Detailed information, including procedural guidelines, technical specifications, and compliance requirements, are outlined in the **Annexure-B** to this policy for reference and implementation."

9.3. **Digital KYC Procedure:**

9.3.1. SCML shall allow customers to complete KYC procedures digitally, leveraging technology platforms in line with RBI's Digital KYC framework.

9.3.2. The process shall involve:

9.3.2.1. Submission of Aadhaar (voluntary) or OVDs in electronic form.

9.3.2.2. Verification of documents through QR code scanning or equivalent digital means, ensuring compliance with IT Act standards.

9.3.2.3. Capturing a live photograph of the customer and matching it with the photo on the OVD.

9.3.2.4. Ensuring that the customer's declaration and consent are captured electronically.

9.3.2.5. The digital KYC process shall use secure and encrypted systems to ensure the integrity and confidentiality of customer data.

9.3.2.6. "Detailed information, including procedural guidelines, technical specifications, and compliance requirements are outlined in the **Annexure-C** to this policy for reference and implementation."

9.4. General Guidelines for CIP:

9.4.1. In all cases, customer identification shall be conducted with the explicit consent of the customer.

9.4.2. Records of all CIPs, including digital logs and video recordings, shall be maintained in a centralized database for periodic review and audit.

9.4.3. SCML shall ensure compliance with relevant data protection laws, including the safeguarding of customer information.

9.4.4. Exceptions, if any, shall be approved by the Designated Director and recorded for supervisory review.

9.4.5. Specific and explicit consent must be obtained from the customer for authentication using Aadhaar OTP.

9.4.6. All transaction alerts, OTPs, and other communications must only be sent to the mobile number registered with Aadhaar.

9.4.7. A robust due diligence process, approved by the Board, must be implemented for handling requests to change the registered mobile number in such accounts.

9.4.8. KYC information uploaded to Central KYC Registry (CKYCR) must clearly indicate that the account was opened using OTP-based e-KYC in non-face-to-face mode.

10. Due Diligence Process for Handling Requests to Change Registered Mobile Number

10.1. It shall start with obtaining a written request from the customer and thereafter verifying the identity of the customer through valid KYC documents.

10.2. Perform additional authentication, such as an in-person visit, video KYC, or a one-time password (OTP) verification sent to both the existing and the new mobile numbers.

10.3. Cross-check the new mobile number with internal records to ensure it is not linked to other accounts fraudulently.

10.4. Require customers to submit supporting documents, such as proof of ownership of the new mobile number (e.g., mobile bill or operator confirmation).

10.5. Route the request through a defined approval hierarchy, ensuring review and approval by a senior officer or designated authority.

10.6. Maintain an audit trail of the request, approvals, and any communications with the customer including notifying the customer once the registered mobile number has been updated successfully.

11. Customer Due Diligence (CDD)

11.1. SCML shall establish a comprehensive CDD framework in compliance with the PMLA and directions issued by the RBI. This framework ensures the identification and verification of customers using reliable and independent sources of identification to mitigate risks of money laundering, terrorism financing, and other financial crimes.

Key Components of Customer Due Diligence (CDD) are:

Customer Identification and Verification	• Identifying and verifying the identity of customers through reliable and independent sources, including government-issued documents (e.g., PAN, Aadhaar, passport). • Collecting information about the purpose and intended nature of the business relationship, where applicable.
Understanding Customer Business and Control	• Taking reasonable steps to understand the nature of the customer's business operations. • Establishing the ownership and control structure for entities or complex account relationships to identify key stakeholders.
Ongoing Monitoring	• Conducting periodic reviews of customer accounts to ensure alignment with their risk profile, declared business activities, and expected transaction patterns. • Detecting, investigating, and documenting unusual or suspicious transactions for further action, including filing Suspicious Transaction Reports (STRs) where required.

Additional Measures for High-Risk Customers	• EDD shall be performed for high-risk customers, including obtaining additional information about their source of funds, business activities. • Senior management approval shall be obtained for establishing or continuing relationships with high-risk customers

12. CDD: Procedure & Implementation Framework

12.1. SCML shall adhere to the following guidelines while conducting CDD in compliance with the PMLA, 2002, and directions issued by the RBI.

12.2. SCML shall obtain the following documents from an "individual" customer when establishing an account-based relationship or dealing with an authorized signatory, or power of attorney holder for any legal entity:

12.2.1. Aadhaar-Based Identification:

12.2.1.1. When the customer is desirous of receiving benefits or subsidies under schemes notified under *Section 7 of the Aadhaar Act*, 2016.

12.2.1.2. If the customer voluntarily provides the Aadhaar number.

12.2.2. Proof of Possession of Aadhaar Number:

12.2.2.1. Where offline verification is possible.

12.2.2.2. Where offline verification is not possible, or any OVD or its equivalent e-document containing identity and address details.

12.2.3. KYC Identifier: With explicit consent to retrieve records from the Central KYC Records Registry (CKYCR).

12.2.4. The PAN or its equivalent e-document, or Form 60 as defined in the Income-tax Rules, 1962.

12.2.5. Documents relevant to the customer's nature of business and financial status, or equivalent e-documents as deemed necessary.

12.3. Verification Process: SCML shall verify the submitted documents through the following methods:

12.3.1. E-KYC Authentication: Aadhaar-based authentication using the Unique Identification Authority of India (UIDAI) e-KYC facility. Customers may submit a self-declaration if their current address differs from the one in the Aadhaar database.

12.3.2. Offline Verification: For proof of possession of Aadhaar where offline verification is possible.

12.3.3. Digital KYC: Verification through live photos and digital signature validation for e-documents or OVDs as per the Information Technology Act, 2000.

12.3.4. Retrieval from CKYCR: Using the KYC Identifier, SCML shall download the KYC records from CKYCR.

12.3.5. SCML may adopt any of the abovementioned methods for KYC verification.

12.4. When a customer submits proof of possession of an Aadhaar number, SCML shall ensure the Aadhaar number is redacted or blacked out where authentication is not required.

12.5. SCML shall maintain records of all CDD activities, including exception handling cases, in compliance with the RBI Directions. The records shall undergo regular audits and inspections to ensure compliance with regulatory requirements.

12.6. The list of documents required to establish the identity and operational existence of different categories of customers including individual shall be annexed to this policy and referred to as **Annexure-D**.

12.7. The KYC Request Form for Non-Individual Clients (Legal Entity), as provided in **Annexure-E** of this policy, outlines the

mandatory information and documentation requirements for onboarding legal entities in compliance with applicable regulatory guidelines. However, the required information and documentation may also be sourced from other valid and reliable sources, including but not limited to publicly available regulatory databases, statutory filings, government portals, or authenticated third-party verification services, provided such sources are credible, current, and verifiable. Where the requisite information is not available through any such alternate valid source, the KYC Request Form prescribed under Annexure-E shall be the primary instrument for collection of such information and documentation.

13. Monitoring of Transactions/On-going Due-Diligence

13.1. SCML shall perform ongoing due diligence to ensure customer transactions align with:

13.1.1. The Company's understanding of the customer,

13.1.2. The customer's declared business activities and risk profile, and

13.1.3. The source of funds or wealth.

13.2. The following transactions shall be subject to close monitoring:

13.2.1. Large and complex transactions, that are inconsistent with the customer's typical activity or lack apparent economic rationale.

13.2.2. Transactions exceeding thresholds prescribed for specific categories.

13.3. A risk-based approach to monitoring accounts shall be adopted, including:

13.3.1. High-Risk Accounts: Intensified monitoring based on their risk category.

13.3.2. Risk categorization review at least every six months for enhanced due diligence.

13.4. SCML may adopt advanced monitoring tools, including Artificial Intelligence (AI) and Machine Learning (ML), to strengthen its ongoing due diligence and ensure compliance with regulatory requirements.

14. Updation/Periodic KYC Updation

14.1. SCML shall adopt a risk-based approach to ensure periodic updation of KYC information, keeping the CDD data accurate and relevant.

14.2. Periodicity of KYC Updation

Type of Customers	Periodic updation of KYC
High-Risk Customers	Carried out at least once every two years from the date of account opening or the last KYC updation
Medium-Risk Customers	Periodic updation of KYC shall be carried out at least once every eight years from the date of account opening or the last KYC updation.
Low-Risk Customers	Periodic updation of KYC shall be conducted at least once every ten years

14.3. KYC Updation for Individuals:

14.3.1. No Change in KYC Information: If there is no change in the customer's KYC information, SCML shall obtain a self-declaration from the customer through any of the following:

14.3.1.1. Registered email ID

14.3.1.2. Registered mobile number

14.3.1.3. Digital channels (e.g., online banking, mobile application)

14.3.1.4. Letter, or other designated modes

14.3.2. Change in Address: For a change in address, the customer shall provide a self-declaration of the new address. SCML shall verify the declared address through positive confirmation within two months using methods such as:

14.3.2.1. Address verification letters

14.3.2.2. Contact point verification

14.3.3. SCML may also obtain a copy of an OVD, deemed OVD, or equivalent e-document for proof of address.

14.3.4. Aadhaar OTP-based e-KYC in non-face-to-face mode may be used for periodic KYC updation, provided the Aadhaar-registered mobile number matches the one in SCML's records.

14.4. KYC Updation for non-individuals:

14.4.1. No Change in KYC Information: A self-declaration shall be obtained from the customer, supported by:

14.4.1.1. Official communication via the registered email ID

14.4.1.2. Digital channels (e.g., mobile application)

14.4.1.3. Letter from an authorized official or board resolution

14.4.2. Change in KYC Information: SCML shall perform KYC equivalent to the onboarding process for new non-individual customers in cases of any changes to the KYC information.

14.5. SCML shall ensure that the KYC documents comply with the current CDD standards and shall undertake KYC equivalent to the onboarding process if:

14.5.1. The validity of CDD documents has expired.

14.5.2. Existing documents are not compliant with current CDD standards.

14.6. The customer's PAN or equivalent e-document shall be verified from the issuing authority during periodic KYC updation.

14.7. SCML shall provide an acknowledgment to the customer upon receipt of documents or self-declarations, indicating the date of receipt and completion of KYC updation.

14.8. Customers shall be advised to inform SCML of any changes to their documents submitted at the time of account opening or thereafter, within 30 days of such changes. SCML shall promptly update its records and notify the customer of the KYC updation date.

14.9. SCML shall ensure that customers can update their KYC information at any branch or through authorized digital channels.

14.10. If a customer fails to provide their PAN, equivalent e-document, or Form 60 within the time prescribed by the Central Government, SCML shall temporarily suspend account operations. However:

14.10.1. The customer shall be given prior notice and a reasonable opportunity to comply.

14.10.2. Credits shall be allowed in asset accounts such as loan accounts during the suspension period.

14.11. Customers unable to provide PAN or equivalent documents due to illness, old age, or other valid reasons may be granted relaxation as deemed appropriate by SCML.

14.12. If a customer refuses to provide PAN, equivalent e-document, or Form 60 in writing, the account shall be closed after settling all obligations and verifying the customer's identity.

15. Enhanced Due-Diligence Measures

15.1. SCML shall adopt Enhanced Due Diligence (EDD) measures in compliance with regulatory requirements for onboarding customers through non-face-to-face channels. These channels include digital methods such as CKYCR, Digi Locker, equivalent e-documents, and non-digital methods such as obtaining a copy

of an OVD certified by additional certifying authorities. Customers onboarded through non-face-to-face methods shall be categorized as high-risk customers. The following EDD measures shall be implemented:

15.1.1. If SCML provides a V-CIP facility, it shall be offered as the primary option for remote customer onboarding. V-CIP processes that comply with the prescribed regulatory standards and procedures shall be considered equivalent to face-to-face customer identification.

15.1.2. To prevent fraud, alternate mobile numbers shall not be linked to customer accounts after the completion of CDD. Transactions shall only be permitted from the mobile number used during account opening.

15.1.3. SCML shall obtain proof of the customer's current address and conduct positive address verification prior to permitting account operations. Verification methods may include address verification letters, contact point verification, or delivery of correspondence to the address.

15.1.4. SCML shall obtain the customer's PAN and ensure its verification using the facility provided by the issuing authority.

15.1.5. Enhanced monitoring measures shall apply to high-risk customers' accounts until the customer's identity is verified through face-to-face interaction or V-CIP.

16. Accounts of Politically Exposed Persons (PEPs)

16.1. This clause establishes the framework for managing relationships with PEPs in compliance with the RBI Master Direction, international guidelines issued by the Financial Action Task Force (FATF), and global AML and Counter-Terrorist Financing (CFT) standards.

16.2. SCML shall implement the following EDD measures when establishing or managing accounts related to PEPs:

16.2.1. Establishing robust risk management systems to identify customers or beneficial owners who qualify as PEPs.

16.2.2. Taking reasonable measures to establish and verify the source of funds and wealth of PEPs.

16.3. Accounts of PEPs, including those of family members and close associates, shall only be opened or continued with the prior written approval of senior management.

16.4. Accounts related to PEPs shall be subject to enhanced monitoring on an ongoing basis. Any unusual or suspicious activity shall be promptly reported to the appropriate regulatory authorities (Financial Intelligence Unit – India (FIU-IND) as required) in accordance with applicable laws in order to mitigate risks associated with corruption, money laundering, or misuse of funds.

17. Record Management

17.1. SCML shall maintain all necessary records of transactions between SCML and its customers, both domestic and international, for a minimum period of five years from the date of each transaction.

17.2. SCML shall preserve records pertaining to the identification and addresses of customers, during the business relationship, and for at least five years after the business relationship has ended.

17.3. Identification records and transaction data shall be made available promptly to competent authorities upon request.

17.4. SCML shall maintain proper records of all transactions as prescribed under *Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.* (https://fiuindia.gov.in/files/AML_Legislation/notification.html#rule_3).

17.5. For customers classified as non-profit organizations, SCML shall ensure their details are registered on the DARPAN Portal of NITI Aayog. If unregistered, SCML shall register the details on the portal. The registration records shall be maintained for a minimum of five years after the business relationship has ended or the account has been closed, whichever is later.

18. Reporting Requirements to FIU-IND

18.1. SCML will submit information required under Rule 3 to the Director, FIU-IND, in line with Rule 7 and adhere to any guidelines issued by the Director regarding reporting and procedures.

18.2. SCML will use the prescribed reporting formats, Report Generation Utility, and Report Validation Utility from FIU-IND for filing Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR). Data from non-fully computerized branches will be consolidated and reported via FIU-IND's electronic utilities.

18.3. All transactions will be reported within the prescribed timelines. Delays or errors beyond the time limit will be treated as separate violations for each day. STR filings will not impose restrictions on account operations.

18.4. SCML and its staff will maintain strict confidentiality regarding records and information shared with FIU-IND, except for sharing analysis or findings related to unusual transactions as required by regulatory guidelines.

18.5. SCML will maintain a robust transaction monitoring system that generates alerts for activities inconsistent with customer profiles or risk categories, ensuring effective identification, analysis, and reporting of suspicious transactions.

19. Combating financing of Terrorism

19.1. SCML shall ensure strict compliance with *Section 51A of the Unlawful Activities (Prevention) Act, 1967*, prohibiting financial transactions with individuals or entities listed under international sanctions. SCML shall not engage in transactions with individuals or entities listed on:

19.1.1. ISIL (Da'esh) & Al-Qaida Sanctions List, accessible at **www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list**.

19.1.2. Taliban Sanctions List, accessible at **https://www.un.org/securitycouncil/sanctions/1988/materials**.

19.1.3. Lists under the *Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007.*

19.2. Sanctions lists shall be reviewed daily for updates. Transactions matching sanctioned entities shall be reported to FIU-IND and the Ministry of Home Affairs (MHA) immediately.

19.3. The procedure prescribed under the Unlawful Activities (Prevention) Act, 1967 (UAPA) Order dated February 2, 2021 (*as specified in Annexure -II of the Scale based regulation Master Direction*), shall be strictly adhered to.

19.4. In addition to the provisions of UAPA, the SCML shall comply with Section 12A of the Weapons of Mass Destruction (WMD) Act, 2005, as per the Ministry of Finance Order dated 01.09.2023, ensuring strict adherence to regulatory requirements. Further, the SCML is committed not to engage in transactions involving individuals or entities listed under Section 12A.

19.5. If a match is found, SCML shall promptly report to the Central Nodal Officer (CNO), with copies to the State Nodal Officer and

RBI. Upon CNO's order, assets shall be frozen immediately. Requests for unfreezing shall be forwarded to the CNO within two working days.

19.6. SCML shall verify the UNSCR 1718 Sanctions List (https://www.mea.gov.in/Implementation-of-UNSC) and other UNSC resolutions daily. Compliance shall be ensured with the First & Fourth Schedules of UAPA and subsequent amendments.

20. Compliance with FATF Recommendations

20.1. SCML shall adhere to FATF Recommendations by identifying high-risk jurisdictions based on RBI-circulated FATF Statements and publicly available information.

20.2. SCML shall apply EDD measures and conduct additional verification before establishing or continuing business relationships with high-risk jurisdictions. Monitor transactions involving such jurisdictions to detect suspicious activities. Transactions shall be permitted only if all regulatory compliance measures are met.

20.3. SCML shall assess and document the background & purpose of high-risk transactions. Retain written findings and supporting documents for regulatory inspections. Provide information to RBI and relevant authorities upon request.

21. Confidentiality of Customer Information

21.1. SCML shall ensure strict confidentiality of customer information obtained through contractual relationships, maintaining the highest level of secrecy except as permitted by this policy.

21.2. Customer data shall not be used for cross-selling or other purposes without explicit consent. Information collected for

account opening or legitimate purposes shall be treated as confidential.

21.3. Disclosures to government agencies or authorities shall comply with legal provisions and confidentiality laws.

21.4. Information shall only be disclosed under the following exceptions:

21.4.1. Mandated by law or regulations.

21.4.2. In the interest of public duty.

21.4.3. For the legitimate interest of the Company.

21.4.4. With the express or implied consent of the customer.

21.5. SCML shall uphold customer privacy rights while ensuring compliance with legal and regulatory requirements.

22. KYC Data Collection and Sharing with CKYCR

22.1. In accordance with the *Government of India's Gazette Notification No. S.O. 3183(E) dated November 26, 2015*, the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) has been authorized to function as the Central KYC Records Registry (CKYCR).

22.2. As per Rule 9(1A) of the PML Rules, SCML shall ensure that customer KYC records are captured and uploaded to the CKYCR within 10 days of establishing an account-based relationship with the customer.

22.3. SCML shall adhere to the operational guidelines released by CERSAI for the uploading of KYC data, which shall be performed in the prescribed manner and within the specified timelines.

22.4. SCML shall capture and upload KYC information in accordance with the KYC templates provided by CERSAI for 'Individuals' and 'Legal Entities' (LEs).

22.5. For individual accounts opened on or after January 1, 2017, and for accounts of Legal Entities (LEs) opened on or after April

1, 2021, the Company shall upload KYC data to CKYCR within the timelines prescribed by CERSAI.

22.6. Upon generation of the KYC Identifier by CKYCR, SCML shall ensure that the KYC Identifier is communicated to the respective customer (individual or LE), as applicable.

22.7. During the periodic KYC update process, SCML shall ensure that customers' KYC records are updated to reflect the current CDD standards. The Company shall upload the updated KYC data to CKYCR within seven days of receiving new or updated information from the customer.

22.8. For account opening, verification of customer identity, or periodic updates, SCML shall retrieve the KYC Identifier from CKYCR (if available) and use it to obtain the customer's KYC records online. The Company shall not require customers to submit the same KYC records unless:

22.8.1. There is a change in the customer information as per the records in CKYCR.

22.8.2. The KYC data retrieved is incomplete or not aligned with current KYC norms.

22.8.3. The validity period of the documents retrieved has expired.

22.8.4. The Company determines it necessary for the purpose of verifying customer identity, address, or performing enhanced due diligence.

22.9. If any discrepancies are identified in the KYC records obtained from CKYCR or if new information is provided by the customer, SCML shall ensure that the updated KYC information is uploaded to CKYCR in accordance with the timelines prescribed. SCML shall retrieve and apply the updated KYC data provided by CKYCR to maintain compliance with KYC and AML regulations.

23. Implementation of Emerging Technologies

23.1. SCML shall assess and mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) when introducing new products, services, or technologies including conducting an ML/TF risk evaluation before introducing or modifying any offering, Implementing EDD, transaction monitoring, and risk controls based on identified risks and regularly monitoring and reassessing risks from emerging technologies.

24. Know your employee standards

24.1. SCML has implemented a separate robust **Know Your Employee (KYE) Policy** as part of its recruitment to ensure employees meet high ethical and integrity standards in order to fulfil KYC/AML/CFT tasks.

25. Monitoring of Suspicious Transactions

25.1. SCML adopts a risk-based approach to monitor transactions for compliance with KYC/AML/CFT regulations and detect suspicious activities.

25.2. A Transaction Monitoring System is in place to flag deviations from customer profiles or unusual patterns indicating money laundering, terrorist financing, or fraud. Red flag indicators are defined based on customer risk, transaction patterns, and industry practices, updated periodically.

25.3. Suspicious transactions are escalated to the Principal Officer for review and reported to FIU-IND as required. Further, internal audits and compliance reviews are conducted regularly to assess and improve monitoring effectiveness.

25.4. Employees in transaction processing, compliance, and risk management are trained to identify & report suspicious activities.

25.5. An indicative list of suspicious transactions is included in **Annexure – F** of the Policy.

Annexure-A: Details of Designated Director and Principal Officer

Position	Name	Designation	Address	Contact details
Designated Director				
Principal Officer				

Annexure-B: V-CIP

The Company shall adopt and implement the Video-Based Customer Identification Process (V-CIP) as a seamless and secure digital alternative to the physical face-to-face process, to fulfil CDD requirements in compliance with applicable regulatory guidelines.

Applicability	Individual Customers: V-CIP shall be used for onboarding new individual customers and for conducting periodic KYC updates. Non-Individual Customers: The process shall be applicable for: • Proprietors of proprietorship firms (with proof of business activity). • Authorized signatories of Legal Entities (LEs).
Customer Consent	Prior to initiating the V-CIP, explicit consent shall be obtained from the customer, in accordance with regulatory guidelines.

Infrastructure and Security Standards	The V-CIP infrastructure shall: • Comply with the baseline cybersecurity and resilience framework issued by RBI. • Be hosted on secured premises or company-secured cloud servers, ensuring sole ownership of data remains with the company. • Incorporate end-to-end encryptions for all interactions between the customer's device and the V-CIP application. • Employ advanced technologies such as: 1. Geo-tagging of interactions. 2. Liveness detection and face-matching algorithms to mitigate vulnerabilities or fraudulent attempts. 3. Restrict access from IP addresses outside India and prevent connections from spoofed Ips.
V-CIP Procedure	The V-CIP process shall be conducted by trained and authorized officials of the company, ensuring the following: • Record audio-video and capture a photograph of the customer present for identification. • Obtain identification information through any one of the following: o OTP-based Aadhaar e-KYC authentication o Offline Aadhaar verification. o KYC records downloaded from CKYCR using the KYC identifier provided by the customer. o Equivalent e-documents of Officially Valid Documents including documents issued through Digi Locker.
Verification Process	• Perform live video interaction to confirm customer identity and conduct real-time liveness checks.

	• Capture a live photo and match it against PAN, Aadhaar, or other OVDs with a threshold accuracy percentage set by the Risk and RCU team. • Verify PAN using authorized APIs and Aadhaar XML not older than three days. If Aadhaar address differs, additional documents for address proof shall be collected.
Failure or Termination	Any disruption in the V-CIP process shall result in immediate termination, with an option to reinitiate the process or switch to the physical KYC process
Records and Data Management	• Data Storage: All V-CIP-related data, including audio-video recordings, logs, and credentials, shall be securely stored within India with proper date and time stamps for audit purposes. • Data Masking: Aadhaar numbers and sensitive customer information shall be masked/redacted as per regulatory requirements. • Audit Trail: A robust audit trail shall be maintained, including activity logs and credentials of officials performing the process.
Compliance and Risk Mitigation	• The company shall conduct periodic Vulnerability Assessments (VA) and Penetration Testing (PT) by CERT-In empanelled auditors, if it is required. • A clear workflow for V-CIP shall be documented, incorporating regulatory requirements to minimize errors and prevent fraud. • Any fraudulent identity case detected during V-CIP shall be reported as a cyber security incident.
Employee Training	All officials executing V-CIP shall undergo: • Regular training on fraud detection, liveliness checks, and customer interaction.

	• Updates on regulatory requirements and advanced V-CIP technologies.
Periodic System Testing	The V-CIP system shall undergo: • Regular vulnerability assessments and penetration testing (VAPT) to ensure robustness and compliance. • Periodic reviews and updates to align with regulatory changes and address emerging risks.

Annexure-C: Digital KYC Process

This clause outlines the steps, requirements, and protocols for the Digital KYC process, ensuring compliance, security, and accuracy while onboarding customers digitally:

Application Development and Availability	• The company shall develop and implement a secure application for conducting the Digital KYC process. • This application shall be made available at customer touchpoints and shall be the sole authenticated platform for carrying out KYC procedures for customers. • The company shall ensure that the application is continuously updated and compliant with all regulatory requirements.
Access Control to Application	• Access to the Digital KYC application shall be restricted to authorized officials of the company. • Access to the application shall be controlled through a login ID and password or an OTP-based system (Live OTP/Time OTP mechanism). • Unauthorized individuals shall not be granted access to the application.

Customer Interaction for KYC Process	• The customer, for KYC purposes, must either visit the authorized official's location or be visited by the authorized official. • The customer must possess the original OVD during the process for verification.
Live Photograph of Customer	The authorized officer shall ensure the capture of a live photograph of the customer during the KYC process. The captured photograph shall be embedded in the Customer Application Form (CAF) containing CAF number, GPS coordinates, Authorized official's name, Unique employee code, Date (DD:MM: YYYY), Time stamp (HH:MM:SS).
Live Photograph Capture Specifications	• The system shall allow only live photographs to be taken and prevent the use of pre-recorded or video-graphed images. • The background behind the customer must be of a white colour to avoid any distractions.
Document Photograph and Watermarking	• The live photograph of the original OVD (or Aadhaar proof if offline verification is not applicable) must be captured from above in a vertical orientation. • The system shall apply watermarking to the photograph, including all details specified above.
Light and Readability Standards	• Both the customer's photograph and original document should be captured in adequate lighting to ensure clarity and legibility to ensure verification.
Auto-Population Using QR Code	• Where available, QR codes in documents (e.g., Aadhaar/e-Aadhaar) shall be scanned, and details such as name, gender, date of birth, and address will be auto-populated into the CAF.

OTP Verification for Customer's Consent	• Upon completion of document verification, an OTP message shall be sent to the customer's registered mobile number with the message: "Please verify the details filled in form before sharing OTP." • The customer must validate the OTP. Upon successful validation, the OTP will act as the customer's electronic signature on the CAF. • If the customer does not have their own mobile number, a family member or a known person's mobile number can be used, provided it is explicitly mentioned in the CAF. • The mobile number of the authorized officer shall not be used for customer verification.
Authorized Officer's Declaration and OTP Validation	• The authorized officer must provide a declaration confirming the capture of the customer's live photograph and the original document. • The officer's identity must be verified via OTP sent to their mobile number registered with the company. • Upon successful OTP validation, the officer's OTP will serve as their electronic signature on the declaration. • A live photograph of the officer shall be captured and embedded in the declaration.
Process Completion and Activation Request	• Upon completion of all KYC steps, the system will notify the activation officer regarding the successful submission and activation request. • A transaction ID/reference number will be generated, which the authorized officer will share with the customer for future reference.

Verification by Authorized Officer	The authorized officer must verify: • The information in the document matches the details entered in the CAF. • The live photograph of the customer matches the image on the document. • All mandatory fields in the CAF are filled correctly and completely.
CAF Signing and Submission	• Upon successful verification, the authorized officer shall digitally sign the CAF. • The CAF will be printed, and the customer's signature/thumb impression will be obtained at the designated place in the form. • The signed CAF shall be scanned and uploaded into the system for final record-keeping. • The original hard copy of the CAF may be returned to the customer as per their request.

Annexure-D: List of Required Documents for CDD

KYC Documents for an account of an Individual
KYC Documents for an Account of INDIVIDUAL, (including Authorized Signatory and Power of Attorney Holder): o One recent Photograph, o PAN or Form 60 if PAN is not allotted o Certified Copy of one of the OVDs.
KYC Documents for Sole Proprietary Firms
CDD of the individual proprietor shall be carried out in accordance with the KYC guidelines. In addition to the proprietor's KYC documents for Individual mentioned above,

1. Any one of the following documents, or their equivalent e-documents, as proof of business/activity in the name of the proprietary firm, shall also be obtained:
    - Registration certificate, including Udyam Registration Certificate (URC) issued by the Government
    - Certificate/licence issued by municipal authorities under the Shop and Establishment Act
    - Sales and income tax returns
    - CST/VAT/GST certificate
    - Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
    - Importer Exporter Code (IEC) issued by the Directorate General of Foreign Trade (DGFT) or license/certificate of practice issued by any professional body incorporated under a statute
    - Complete Income Tax Return (not just the acknowledgment) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by Income Tax authorities
    - Utility bills such as electricity, water, landline telephone bills, etc.
2. In cases where it is not feasible to furnish two such documents, the company may, at their discretion, accept one document as proof of business/activity, provided the company undertake contact point verification and collect additional information and clarification necessary to establish the existence of the firm.

KYC Documents for Companies

Certified copies of the following documents, or their equivalent e-documents, shall be obtained:

- Certificate of incorporation
- Memorandum and Articles of Association
- PAN of the company
- Board resolution and power of attorney granted to its officers, managers, or employees to transact on its behalf

o Documents of Individual, related to beneficial owners, managers, officers, or employees holding authority to transact on the company's behalf o Names of the relevant persons holding senior management positions o Registered office and principal place of business, if different
KYC Documents for Partnership Firms
Certified copies of the following documents, or their equivalent e-documents, shall be obtained: o Registration certificate o Partnership deed o PAN of the partnership firm o Documents of Individual, related to managers, officers, or employees holding authority to transact on the firm's behalf o Names of all partners o Registered office address and principal place of business, if different
KYC Documents for Trusts
certified copies of the following documents, or their equivalent e-documents, shall be obtained: o Registration certificate o Trust deed o PAN or Form No. 60 of the trust o Documents of Individual, related to managers, officers, or employees holding authority to transact on the trust's behalf o Names of the beneficiaries, trustees, settlor, protector (if any), and authors o Registered office address of the trust o List of trustees and relevant documents for trustees authorized to transact on behalf of the trust
KYC Documents for Unincorporated Associations/Body of Individuals **Unregistered trusts and partnership firms shall be included under the term 'unincorporated association.'*

**The term 'body of individuals' includes societies.*
Certified copies of the following documents, or their equivalent e-documents, shall be obtained: o Resolution from the managing body of such an association or body of individuals o PAN or Form No. 60 of the unincorporated association or body of individuals o Power of attorney granted to transact on its behalf o Documents, as specified in paragraph 16, relating to beneficial owners, managers, officers, or employees holding authority to transact on its behalf o Other information necessary to establish the legal existence of the association or body of individuals
KYC Documents for Other Juridical Persons (such as societies, universities, local bodies, etc.)
Certified copies of the following documents, or their equivalent e-documents, shall be obtained: o Document showing the name of the person authorized to act on behalf of the entity o Documents of Individual, related to the person holding authority to transact on behalf of the entity o Other necessary documents to establish the legal existence of the entity/juridical person

Annexure-E: KYC Request Form for Legal Entity

[To be printed on the letterhead of the Borrower]

Date _____

Sub: KYC Details

Name of the Customer (Borrower)	
Date of Incorporation	
Place of Incorporation	
Country of Incorporation	
Date of Commencement of Business	
Country of Residence as per Tax laws	
Nature of Application (Private Limited Company, Public Limited Company, Trust, Society, Partnership, NGO, Government Aided Institution, NBFC, HFC, Producer Company, Others. If 'Others' please specify exact nature)	

Proof of Identity: a) Certificate of Incorporation; b) Memorandum of Association; and c) Articles of Association	

Section 1: Customer Identity Details

Section 2: Address and Contact Details

Registered Office Address along with a proof of address (Form INC-22 OR Form 18 filed with ROC along with challan, OR MCA master data print out certified by Director/CFO/CS)	
Correspondence Address, *if different from Registered Office Address, then proof of address to be submitted (latestutility bill or bank account statement)*	
Phone Number	
Mobile Number	
Fax Number	
Email ID	
Principal Place of Business(es)	

Section 3: Statutory Registration

CIN (Applicable to Company only)	
Entity Registration Number (Applicable to entities other than a Company)	
Permanent Account Number (PAN)	
GST Registration Number	
If registered for Tax Purposes in Jurisdiction Outside India: Tax Identification Number (TIN)	
If registered for Tax Purposes in Jurisdiction Outside India: TIN Issuing Country	

Section 4: Authorized Signatory(ies) and Beneficial Owner(s)[1]

Name (same as ID proof)	
Maiden Name (If any)	
One recent photograph	
Father / Spouse Name (tick which is applicable)	

Mother Name	
Date of Birth	
Gender (Male / Female / Transgender)	
Marital Status (Married / Unmarried / Others)	
Residential Status (Residential Individual, Non-Residential Individual, Foreign National, Person of Indian Origin)	
If Resident for Tax Purposes in Jurisdiction(s) Outside India - please provide below details if applicable: a. Country of Jurisdiction of Residence: b. Tax Identification Number or equivalent (If issued byjurisdiction): c. City of Birth: d. Country of Birth:	
e. Passport number:	
Occupation Type: a. Service / Business / Others b. Private Sector/Professional/Public Sector/Government Sector/Self Employed/Retired/Housewife/Student/Not Categorized	
PAN no. along with PAN Card copy	
Permanent Address along with proof (Aadhaar Card / Passport / Driving License / Voter ID)[2]	
Current residence Address along with proof (Aadhaar Card / Passport/ Driving License / Voter ID)	
Phone Number	
Mobile Number	
Fax Number	
Official Email ID	
Relationship of Authorized Signatory with the Customer (Management / Director/ Promoter/Beneficiary/Court Appointed Official / Other)	
Copy of Board Resolution for authorization of signatory	

Declaration

I/We hereby declare that the details furnished above are true and correct to the best of my/our knowledge and belief and I/we undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am/we are aware that I/we may be held personally liable for it. My/Our personal KYC details may be shared with Central KYC Registry. I/We hereby consent to receiving information from Central KYC Registry through SMS/Email on the above registered number/email address.

For and on behalf of [____]

Name: [_____]

Designation: [_____]

Annexure-F: (Indicative List of Suspicious Transactions)

In pursuance of the statutory and regulatory guidelines, Activities which are not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.

The following shall be construed as suspicious transactions/activities:

1. **Transactions Involving Large Amounts of Cash:** SCML transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques.
2. **Transactions that do not make Economic Sense:** Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnish a plausible reason for immediate withdrawal.

3. **Activities not consistent with the Customer's Business:** Accounts with large volume of credits whereas the nature of business does not justify such credits.

4. **Attempts to avoid Reporting/Record-keeping Requirements:**

4.1. 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.

4.2. Any individual or group that coerces/induces or attempts to coerce/induce a SCML employee not to file any reports or any other forms.

4.3. An account where there are several cash transactions below a specified threshold level to a 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.

5. **Unusual Activities:** Funds coming from the countries/centres which are known for money laundering.

5.1. Customer who provides Insufficient or Suspicious Information:

5.1.1. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.

5.1.2. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

5.1.3. A customer who has no record of past or present employment but makes frequent large transactions.

6. **Certain SCML Employees arousing Suspicion:**

6.1. An employee whose lavish lifestyle cannot be supported by his or her salary.

6.2. Negligence of employees/wilful blindness is reported repeatedly.

7. **Some examples of suspicious activities/transactions to be monitored by the operating staff:**

7.1. Large Cash Transactions

7.2. Multiple accounts under the same name

7.3. Placing funds in term Deposits and using them as security for more loans

7.4. Sudden surge in activity level

7.5. Same funds being moved repeatedly among several accounts.