SRINIDHI CREDIT PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC) POLICY

INDEX

S.NO.	SUBJECT	PAGE NO.
1	Preamble	1
2	Objectives, Scope and Application of the policy	1
3	Definitions	2
4	Money laundering (ML) and Terrorist financing (TF) risk assessment	4
5	Key elements	4
	5.1. Customer Acceptance Policy("CAP")	4
	5.2. Customer Identification Procedures ("CIP")	5
	5.3. Monitoring of transactions	7
	5.4. Risk Management	9
6	Training Programme	11
7	Internal Control System	11
8	Record keeping	11
9	Appointment of Designated Director and Principal Officer	12
10	General	13
11	Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) reporting:	14
12	Reporting to Financial Intelligence Unit – India	14
13	Annexure - 1	15
14	Annexure - 2	16
15	Annexure - 3	19

KNOW YOUR CUSTOMER' POLICY

1. Preamble:

Money Laundering is the process of concealing financial transactions to make illegitimate money, derived from illegal activities such as embezzlement/ corruption/ illegal gambling/ terrorism/ organized crime, appear legitimate. Its main objective is to hide the true source of illegal proceeds and make them legally usable, by converting them into legitimate money through a series of financial transactions. Technological advancements have helped money launderers adopt innovative means to transfer funds faster across continents making detection and preventive action more difficult. The attempted misuse of the financial system for perpetration of frauds has been recognized globally as a major problem that needs to be continuously tackled at every level in a dynamic manner. Our role in curbing this global reality begins with stringent Know Your Customer procedures.

In the light of the guidelines issued by Reserve Bank Of India and updated from time to time a standardized and uniform policy framework has been adopted by Srinidhi Credit Private Limited ("SCPL"/ "Company") to ensure appropriate customer identification and monitoring of unusual/ suspicious transactions on an ongoing basis. It aims at preventing the Non-Banking Finance Company's (NBFC's) from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism.

Accordingly, the following KYC Policy has been duly approved by the Board of Directors of SCPL. The Board shall review this Policy at least annually or as and when required pursuant to regulatory changes as notified by RBI from time to time.

2. Objectives, Scope and Application of the policy:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better, which in turn will help it to manage its risks prudently.

Thus, the KYC policy has been framed by the Company for the following purpose:

- To enable SCPL to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage its risks prudently.
- To prevent criminal elements from using SCPL for money laundering activities.
- To comply with applicable laws and regulatory guidelines.
- To ensure that the concerned staff are adequately trained in Know Your Customer (KYC) /Anti Money Laundering (AML) /Combating Financing of Terrorism (CFT) procedures.
- To establish a robust control framework comprising internal checks, monitoring mechanisms and governance oversight to mitigate risks of financial fraud, money laundering and terrorist financing, and to ensure the Company is not used as a conduit for unlawful financial activities.

3. Definitions

3.1 **Customer** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.2 **Walk-in Customer** means a person who does not have an account-based relationship with the RE, but undertakes transactions with the Company.

3.3 **Customer Due Diligence/ (CDD)** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

3.4 **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.

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

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

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

3.8 **"PML Act"** shall mean the Prevention of Money Laundering Act, 2002.

3.9 **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.

3.10 **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 RE 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, including mandatory capture of live location (latitude and longitude), end-to-end encrypted transmission, secure storage, and periodic independent audit as prescribed by RBI (NBFC- KYC) Directions, 2025.

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

3.12 **Officially Valid Document /(OVD)**: shall have the meaning assigned under Rule 2(1)(d) of the Prevention of Money Laundering Rules, 2005, updated from time to time ("PML Rules") and as adopted under RBI (NBFC – KYC) Directions, 2025.The following documents as mentioned in OVD shall be obtained from all Customers;

Sl.NO	KYC Document	ID Proof	Sign Proof	Address Proof	Age proof
1	Passport	Yes	Yes	Yes	Yes
2	Voter ID Card	Yes	No	Yes	Yes
3	Driving License	Yes	Yes	Yes	Yes
4	Job card issued by NREGA duly signed by State govt office customer	Yes	No	No	Yes
5	Letter issued by National Population Register	Yes	No	Yes	Yes

6	Proof of possession of Aadhaar (As per UIDAI, AADHAR card can be used as OVD only on masking the number)	Yes	No	Yes	Yes

Mandatory Document: PAN shall be mandatory for Customers as per Rule 114B of Income Tax Rules, 1962. In the absence of PAN, Form 60 shall be accepted for the customers. However, the income validation has to be performed in line with the income declared in Form 60.

Self-declaration shall be obtained in case the current address differs from the address in OVD.

3.12.1. If 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;

- Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill;
- Property or Municipal Tax receipt;
- Bank account or Post Office savings bank account statement;
- Pension or family Pension payment orders (PPOs) issued to retired employees by Government Departments or PSUs, if they contain address.
- Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and vi. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.

3.12.2. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at (3.13.1) above.

3.12.3. Where the OVD presented by a foreign national (NRI) does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and the letter issued by the Foreign Embassy shall be accepted as proof of address.

3.13 **Principal Officer** means an officer at the management level nominated by the Company, responsible for furnishing information as per Rule 8 of the PML Rules.

3.14 **Reporting Entity** for the purpose of this Policy would mean the Company, Srinidhi Credit Private Limited (SCPL).

3.15 **Equivalent e-document** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer.

4. Money laundering (ML) and Terrorist financing (TF) risk assessment:

4.1 As per the RBI (Non-Banking Financial Company – Know Your Customer (KYC)) Directions, 2025 (as amended from time to time) the KYC policy of the company includes the amendment with regard to Money Laundering and Terrorist Financing Risk Assessment by the Regulated Entities (SCPL).

4.2 SCPL 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.

4.3 Company shall apply a Risk-Based Approach (RBA) and implement a CDD programme regard to ML/TF for mitigation and management of the identified risk and should have Board-approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

5. Key elements

The Policy includes four key elements:

1. Customer Acceptance Policy (CAP)
2. Customer Identification Procedures (CIP)
3. Monitoring of Transactions and
4. Risk management

5.1. Customer Acceptance Policy("CAP")

The Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. SCPL shall ensure that:

5.1.1 No application for financial facilities is accepted in anonymous or fictitious / benami name(s) /entity(ies).

5.1.2 No application is processed where SCPL is unable to apply appropriate Customer Due Diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

5.1.3 Accept customers only after verifying their identity, as laid down in Customer Identification Procedures (as specified in 5.2 point below). Necessary checks before opening a new account are to be ensured so that customers with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. are detected early.

5.1.4 Classify customers into various risk categories, (as specified in 5.4 point below). based on risk perception, apply the acceptance criteria for each category of customers. Parameters of risk perception are clearly defined in terms of nature of business activity, location of customer and his clients, mode of payments, turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk.

5.1.5 The Company shall prepare a credit appraisal note for each customer. The note shall contain information relating to the customer's identity, financial details, nature of business activity and information about their business. The nature and extent of due diligence will depend on the risk perceived by SCPL. These details will be collected from the Loan application. The customer profile document shall not be divulged for cross-selling or for any other purposes. SCPL will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

5.1.6 The company shall apply the CDD procedure at the UCIC (Unique Customer Identification number) level. Thus, if an existing KYC compliant customer of SCPL, desires to open another account there shall be no requirement for a fresh CDD exercise.

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

account. In circumstances where SCPL is unable to apply appropriate Customer Due Diligence (CDD) measures, including inability to verify identity or obtain reliable documents/information, the Company shall not open a new account or disburse any funds.

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

5.1.9 Where Goods and Services Tax (GST) details are obtained, the same shall be verified from the search/verification facility of the issuing authority.

5.1.10 Where Permanent Account Number (PAN) is obtained, the same shall be verified from income tax portal (https://www.incometax.gov.in/iec/foportal/).

5.1.11 Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.to the members.

5.1.12 Customer Acceptance Policy shall not result in denial of financial facility of the general public, especially those, who are financially or socially disadvantaged including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded.

5.1.13 All documentation requirements and other information collection shall be in compliance with the Act and RBI guidelines/instructions.

5.1.14 The Company may rely on third-party verification for customer due diligence, subject to conditions prescribed by the Reserve Bank of India.

5.1.15 Information collected from customers shall be treated as confidential and shall not be disclosed, except as required by law or regulatory authorities.

5.1.16 Optional or additional information may be obtained from the customer only with explicit consent.

5.1.17 The mandatory information sought for KYC purpose while opening an account and during the Periodic Updation, is specified. Any additional information, where such information requirement has not been specified in the Policy herein, will be obtained with the explicit consent of the customer.

5.1.18 Where a suspicion of money laundering or terrorist financing, is formed and reasonably believed that performing the CDD process will tip-off the customer, CDD process shall not be pursued and shall be reported as suspicious transaction to a centralised AML cell for onward reporting of the suspicious transaction to FIU—IND.

5.2. Customer Identification Procedures ("CIP")

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information in the CDD process. SCPL shall obtain sufficient information necessary to verify the identity of each new customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of Business relationship.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.) as specified in **Annexure 2**.

An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure 2**. SCPL shall carry out identification procedure at different stages, i.e., while establishing a relationship; carrying out a financial transaction or when

there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

5.2.1. Verification

Verification of customer identity shall occur before transacting with the customer. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents or non-documentary verification methods that are appropriate and the associated risks as below. The Company will implement procedures to communicate and resolve information discrepancies and, if not resolved, to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence.:

5.2.1.1. CKYCR

CKYCR is an entity under CERSAI to receive, store, safeguard and retrieve the KYC records in digital form of a customer. CKYCR manages the KYC for Individual and Legal Entities.

- Sharing of information to CKYCR
    - Upload KYC record of the customer within 10 (ten) days of commencement of an account-based relation. Whenever SCPL receives updated or additional information of the customer pursuant to Periodic Updation or otherwise, such information shall be uploaded, as per Paragraph 63(7) of the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, within 7 days of receipt or such other timeline as may be prescribed under applicable law.
    - Applicable operational guidelines issued by CERSAI for uploading the KYC data shall be followed.
    - During Periodic Updation, the customers are migrated to the current CDD standards (KYC documentation and information).

Use of Information from CKYCR

With an explicit customer consent and submission of KYC Identifier from the customer or with the help of acceptable digital solutions, the company shall retrieve the KYC records online/download from CKYCR using KYC Identifier.

In such cases, the customer will not be required to submit KYC / OVD document or information or any other additional identification document or detail, unless:

(i) There is a change in the information available in CKYCR;

(ii) the KYC record retrieved is incomplete or not in conformity with current KYC norms;

(iii) the validity period of documents has expired; or

(iv) SCPL considers it necessary to conduct enhanced due diligence or to verify identity/address for risk assessment purposes.

This Provision is subject to following conditions,

- This provision is applicable only for customers falling under Low Risk or Medium Risk category.
- Address as per application form and CKYC documents is same. Additionally, wherever Field Investigation is done, field investigation should confirm the same address.
- The document should be valid at the time of proposed loan and it should be an acceptable KYC document as per the Policy.
- If for any specified reason customer is picked up for additional/enhanced due diligence, then customer Identity and Address shall be verified through appropriate means which may include submission of additional KYC document and personal visit.
- In case contact point verification / customer interaction reports that customer address / KYC detail does not match with the downloaded KYC then fresh KYC shall be obtained.
- Non-Individual customers the documents specified in Annexure II are required afresh from customer / digital source.

5.2.1.2. **<u>CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)</u>:** To ensure that all KYC records are progressively uploaded to CKYCR, SCPL will upload or update KYC information for individual and non-individual (legal entity) customers during the periodic KYC review as prescribed under paragraph 42 of the RBI (NBFC-KYC) Directions, 2025, or earlier whenever updated details are received from the customer. Further, whenever SCPL obtains any additional or revised customer information in accordance with Paragraph 63(7) of the RBI (NBFC-KYC) Directions, 2025, or Rule 9(1C) of the PML Rules, the same shall be submitted to CKYCR within seven days, or within any other timeline specified by the Central Government. CKYCR will then update the existing customer's KYC record accordingly.

CKYCR shall thereafter inform electronically all the reporting entities that have dealt with the concerned customer regarding the updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of;

- an existing customer, SCPL will retrieve the updated KYC records from CKYCR and update the KYC record maintained by SCPL.
- Read with Paragraph 63(7) of the RBI (NBFC-KYC) Directions, 2025, the following is interpreted:

  For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, SCPL shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

(i) there is a change in the information of the customer as existing in the records of CKYCR; or

(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or

(iii) the validity period of downloaded documents has lapsed; or

(iv) SCPL considers it necessary to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

5.3. Monitoring of transactions:

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions will be conducted, taking into consideration the risk profile and risk sensitivity of the account. SCPL shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. SCPL shall monitor high risk category of accounts and pay attention to their transactions.

SCPL shall ensure that books of accounts providing for records of transactions are preserved and maintained (as specified below in point number 8.1) as required in terms of section 12 of the PMLA.

Process for monitoring and reporting of suspicious transactions:

- **Raising suspicion:**

  When the concerned officer has reason to believe that a transaction is/ may be a suspicious transaction, which may be linked with terrorist activity or money laundering, She/he must flag the issue forthwith to the Risk Committee. The concerned officer may consider the following for the purpose of flagging such issue:

  - Amount involved are related to crimes of money laundering, the financing of terrorism, or the financing of illegal organizations.
  - Amount involved are intended to be used in an activity related to such crimes.

- **Identification and evaluation:**

  Once the issue is flagged, formal due diligence is to be conducted to evaluate the suspicion, which shall factor all the attributes and nature of the transaction and in terms of volume, track record, time of transaction, KYC records, behavioral patterns, customer due-diligence information etc. Additional details in relation to a customer can be obtained to substantiate further information. Once proper documentation is obtained and if the concerned officer is satisfied, the issue shall be closed and recorded. Mere presence of an indicator of suspicion does not necessarily always mean that a transaction is suspicious and needs to be reported. When determining whether a transaction is suspicious, consideration to be given to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its due diligence profile. In some cases, patterns of activity or behavior that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another. In case, the concerned officer is not satisfied, it shall be further evaluated or escalated to next level, and will be taken up to Nodal Officer who can analyze the case/report and issue shall be closed or reported.

- **Reporting of suspicious transactions:**

  The Nodal officer may record the reasons of suspicious transactions and evaluate on onward reporting to FIU-IND. Once the Nodal officer is satisfied, that the suspicious transaction is valid and reportable, the same is reported to FIU-IND in accordance with the prescribed

formats. The fact of furnishing of suspicious transactions shall be strictly kept confidential to ensure that there is no tipping off to the customer at any level.

The periodicity of KYC updation:

- Low Risk : Every Ten years
- Medium Risk: Every Eight Years
- High Risk: Every Two Years.

Periodicity of KYC updation for Individual Customers:

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

(ii) Change in address: Company shall obtain a self-declaration of the new address through the customer's email ID registered with the SCPL, customer's mobile number registered with SCPL, ATMs, digital channels (including mobile application of SCPL), letter, etc., and shall verify the declared address through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. The Company may obtain a copy of OVD or deemed OVD or the Equivalent E- documents thereof, for the purpose of proof of new address, declared by the customer at the time of periodic updation.

(iii) Additional measures:

- The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- An acknowledgement is provided to the customer mentioning the date of receipt of the relevant document(s), including a self- declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- Risk based approach for periodic updation of KYC, ensuring that the information or data collected under CDD is kept relevant and up-to-date, particularly for high risk customers.

Due Notices to Customer for Periodic Updation of KYC:

Customers shall be informed in advance regarding the requirement to update their Know Your Customer (KYC) details. At least three advance intimations shall be sent to customers before the due date of periodic KYC updation, including at least one intimation by letter, at appropriate intervals. In the event that the customer fails to update KYC Information, then SCPL shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations.

The following details are to be covered in customer communication, including the intimation and reminders:

- Easy-to-understand instructions for updating KYC
- Details of contacts/ escalation mechanism for customer to update KYC at office.
- The potential consequences should be communicated to customers appropriately in letter/ any other mode. The issuance of all such intimations and reminders must be appropriately recorded in the system for each customer, ensuring a complete audit trail.

6.4 Customer other than individual;

(i) Change in KYC information: SCPL shall obtain an equivalent document in a written letter or via mail. The Company shall obtain OVD as per **Annexure II**.

5.4. Risk Management:

SCPL based on its experience with customers and market information gathered through Credit Information Bureau like (CIBIL) credit ratings, shall over a period of time put in place systems that would enable risk assessment of its customers. Based on the risk assessment, SCPL shall take steps to categorize customers. The customers and their profile shall be reviewed once in every 3months.

5.4.1. Risk Categorization:

The Company has a system in place for periodical updation of customer identification data after the account is opened. In the process of Risk Profiling the Company has a Risk based approach, after taking into consideration the assessment and risk perception of the Company. Each customer is categorized into low, medium and high risk. In this KYC Policy, the term "**risk**" is considered in the context of money laundering and financing terrorism (not credit risk, loan default risk, etc.). Risk profiling of customer is based on customer's identity, social/financial status, nature of business activity, information about the customer business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The Company has adopted the following classification for risk categorizations of its customers.

- Low Risk Category
- Medium Risk Category
- High Risk Category

5.4.2. Indicative List of Risk Categorization:

I. Low Risk Category:

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile are categorized as low risk.

Lower due diligence may include:

(i) Salaried employees with well-defined salary structures;

(ii) People working with government- owned companies, regulators and statutory bodies, etc.;

(iii) People belonging to lower economic strata of the society whose accounts show small balances and low turnover;

(iv) People working with Public Sector Units;

(v) People working with reputed Public Limited Companies and Multinational Companies

II. Medium Risk Category:

Customers are categorized as Medium Risk only when they do not meet the criteria for either Low Risk or High Risk classification.

III. High Risk category:

Customers requiring higher due diligence may include:

(i) politically exposed persons (PEPs) of Indian/foreign origin,

(ii) non-face to face customers, and

(iii) those with dubious reputation as per public information available, etc.

(iv) NRI Customers' if the customers earn Salary in Cash in origin country or employed in Countries that are classified under FATF.

(v) Individuals and entities listed or identified in – various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267, schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.

(vi) Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.

(vii) Gambling/gaming including "junket operators" arranging gambling tours.

(viii) Jewelers and Bullion Dealers.

Customer screening

The risk-assessment process begins with screening customers against the Negative / Freeze Lists. Whenever the Reserve Bank of India circulates any caution list, the Legal / Compliance / Secretarial.

6. Training Programme:

SCPL presently does not have branches. SCPL operates from its office at New No.17, Old No.4, Krishnaswamy Avenue, Mylapore, Chennai - 600004. SCPL shall have an ongoing employee training programs so that the members of the staff at its corporate office are adequately trained

in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for frontline staff, compliance staff and officer/ staff dealing with new customers so that the concerned staff comply with KYC policies and implement them consistently.

The Company shall implement an adequate screening mechanism as part of its recruitment and hiring process. All employees shall undergo training on KYC/AML/CFT guidelines as part of the induction

programme.

The Company shall ensure that personnel handling or deployed for KYC/AML/CFT functions possess high integrity and ethical standards, a sound understanding of prevailing KYC/AML/CFT requirements, effective communication skills, and the ability to stay updated with evolving regulatory developments at both national and international levels. The Company shall also foster a culture of transparency, open communication, and integrity among its staff.

7. Internal Control System:

The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function shall periodically provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

8. Record keeping:

8.1. Maintenance of records of transactions:

The Company shall maintain proper record of the transactions as required under Section 12 of the PML Act read with Rules 3 of the PML Rules as mentioned below:

i. The Company, as a policy, does not accept cash deposits in foreign currency.
ii. All transactions involving receipts by non-profit organizations of Rs. 10 lakhs or its equivalent in foreign currency.
iii. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
iv. All suspicious transactions, whether or not made in cash and in manner as mentioned in the Rules framed by the Government of India under PMLA.
v. Maintenance of records of the identity and address of the customer records in respect of transactions in hard or soft format.

8.2. Information to be preserved:

SCPL shall maintain the record of all transactions (list of transactions are mentioned in annexure III) , shall maintain the following information in respect of transactions referred to in Rule 3 of PMLA.

- the nature of the transactions.
- the amount of the transaction and the currency in which it was denominated.
- the date on which the transaction was conducted.
- the parties to the transaction.

8.3. Maintenance and preservation of records

Section 12 of PML Act requires the Company to maintain records as under:

(i) Records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules are required to be maintained for a period of five years from the date of transactions between the clients and SCPL.

(ii) The said records are to be provided swiftly to Competent Authorities upon request.

(iii) Records of the identity of all clients of SCPL are required to be maintained for a period of five years from the date of cessation of transactions between the clients and SCPL. SCPL shall take appropriate steps to retrieve data easily and quickly whenever required or as/ when requested by the competent authorities.

(iv) The said documents shall be maintained in hard or soft format as per SCPL convenience.

Any other records as prescribed under by any competent authority shall be maintained by SCPL, in accordance with applicable laws, rules, etc.

9. Appointment of Designated Director / Principal Officer:

The Board of Directors shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director". The name, designation and address of the Designated Director shall be communicated to the FIU-IND. As per the RBI guidelines, the Principal Officer is located at our corporate office and is responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He/ She maintains a close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The Company shall publish the contact details of the Principal Officer and/or Designated Director on its website/annual report.

10. General

10.1. Customer Education

SCPL shall at the time of obtaining loan application inform the Customer of the objectives of the KYC Policy so that the Customer understands and appreciates the motive and purpose of collecting such information.

10.2. Introduction of new technologies

SCPL shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering. SCPL shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment.

10.3. Closure of Accounts / Termination of Financing / Business Relationship

Where SCPL is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the customer, SCPL shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of the Board of Directors for the purpose.

10.4. KYC for the Existing Accounts:

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions with existing customers would be continuously monitored for any unusual pattern in the operation of the accounts.

10.5. Updating KYC Policy of Company

Principle Officer after taking the due approval from the Board of Directors of SCPL shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

11. Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) reporting:

In line with regulatory guidelines, all account holder needs to provide a FATCA/ CRS declaration/ self-certification form apart from regular KYC information at the time of on-boarding. A loan account becomes reportable under FATCA/CRS if the account holder/controlling persons are tax residents of any country other than India.

12. Reporting to Financial Intelligence Unit – India:

In accordance with the requirements under PMLA, the Principal Officer of the Company will furnish the necessary reporting i.e Cash Transaction Counterfeit Currency Report, and such other reporting as specified in PMLA, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND).

Annexure 1

Customer Identification Requirements (Indicative Guidelines)

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. SCPL shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, SCPL shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, SCPL shall take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

SCPL shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. SCPL shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. SCPL shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. SCPL shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP shall be taken at a senior level which shall be clearly spelt out in Customer Acceptance policy. SCPL shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms will also be applied to the accounts of the family members or close relatives of PEPs.

Annexure 2

Customer Identification Procedure: Documents to be obtained from Customers.

1. Individuals (Applicant/ Co –Applicant):

Sl.NO	KYC Document	ID Proof	Sign Proof	Address Proof	Age proof
1	Passport	Yes	Yes	Yes	Yes
2	Voter ID Card	Yes	No	Yes	Yes
3	Driving License	Yes	Yes	Yes	Yes
4	Job card issued by NREGA duly signed by State govt officer	Yes	No	No	Yes
5	Letter issued by National Population Register	Yes	No	Yes	Yes
6	Proof of possession of Aadhaar (As per UIDAI, AADHAR card can be used as OVD only on masking the number)	Yes	No	Yes	Yes

Additional Documents required for Individuals:

Sl.No	Particulars	Documents Required
1	Utility Bill for Address Proof	(i) Telephone bill (ii) Bank Account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Letter from employer (subject to satisfaction of the Company) (Any one document which provides customer information to the satisfaction of the Company will suffice)
2	Photograph	One recent passport size photograph except in case of transactions referred to in Rule 9(1)(b) of the PML Rules
3	Declaration	FATCA declaration in case of Non-resident.

2. Companies (Applicant/ Co – Applicant)

Sl.No	KYC Documents
1	Certificate of incorporation
2	Memorandum and Articles of Association.
3	Permanent Account Number of the company.
4	Identification information i.e. PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5	A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
6	Names of the relevant persons holding senior management position
7	Registered office and the principal place of its business, if it is different.
8	GST certificate
9	List of Shareholders
10	FATCA declaration in case of Non- Resident
11	Documents to verify Ultimate Beneficial Owner

3. PartnershipFirms

Sl.No	KYC Documents
1	Registration certificate
2	Partnership deed
3	Permanent Account Number of the partnership firm not as Identification document but as a corroborative document.
4	Identification information i.e. PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5	Identification information i.e. Any document as mentioned in OVD list along with PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
6	GST certificate
7	FATCA declaration in case of Non- Resident
8	Documents to verify Ultimate Beneficial Owner
9	Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses.
10	Other details such as : i) Contact details of Partners ii) Names of all the partners iii) Address of the registered office, and the principal place of its business, if it is different. iv) Identity and address proof of all partners

4. Accounts of Proprietary Concerns

Sl.No	KYC Documents
1	Copy of PAN
2	Any registration / licensing documents issued in the name of the proprietary concern by the Central Government or State Government Authority / Department, IEC (Importer Exporter Code) issued to the Proprietary concern by the office of DGFT as an Identity document for opening of account
3	The complete Income tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated
4	Utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern

5. Trust

Sl.No	KYC Documents
1	Registration certificate
2	Trust deed.
3	Permanent Account Number or Form 60 of the trust.
4	Other details: i) identification information i.e. Any document as mentioned in OVD list along with PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf. ii) Names of the beneficiaries, trustees, settlor and authors of the trust. iii) Address of the registered office of the trust, iv) List of trustees and documents, as specified in Section 16, for those discharging role as trustee and authorized to transact on behalf of the trust

6. Unincorporated association or body of individuals:

Sl.No	KYC Documents
1	Permanent Account Number or Form 60 of association or body of individuals
4	Other details: 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) Such information may be required by the bank to collectively establish the legal existence of such an association or body of individuals

Annexure 3

Rule 3 of PML : Maintenance of records of transactions(nature and value)

(A) all cash transactions of the value of more than ten lakhs rupees or its equivalent in foreign currency;

(B) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

(BA) all transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency;

(C) 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;

(D) all suspicious transactions whether or not made in cash and by way of :

(i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of :

a. cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or

b. traveller's cheques, or

c. transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or

d. any other mode in whatsoever name it is referred to;

(ii) credits or debits into or from any non-monetary accounts such as demat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:—

(a) payment orders, or

(b) cashiers cheques, or

(c) demand drafts, or

(d) telegraphic or wire transfers or electronic remittances or transfers, or

(e) internet transfers, or

(f) Automated Clearing House remittances, or

(g) lock box driven transfers or remittances, or

(h) remittances for credit or loading to electronic cards, or

(i) any other mode of money transfer by whatsoever name it is called;

(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of:

(a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or

(b) purchase and negotiation of bills, cheques and other instruments, or

(c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or

(d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

(v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

(E) all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;

(F) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

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 furnishes a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business.

Accounts with a large volume of credits and the nature of business do not justify such credits.

Attempts to avoid Reporting/Record-keeping Requirements:

i. 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.

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

iii. 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 imit.

Unusual Activities

Funds from countries/centers known for money laundering activities. Customer who provides Insufficient or Suspicious Information

i. 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.

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

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

Certain NBFC Employees arousing Suspicion:

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees/willful blindness is reported repeatedly.

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

- Large Cash Transactions
- Multiple accounts under the same name.
- Placing funds in term Deposits and using them as security for more loans.
- Sudden surge in activity level.
- Same funds being moved repeatedly among several accounts.

****

Revision History

Particulars	Date
Issue Date	16th October, 2017
First Revision Date	17th June, 2023
Second Revision Date	08th December 2023
Third Revision Date	04th January,2024
Forth Revision Date	28th November 2024
Fifth Revision Date	20th June 2025
Sixth Revision Date	20th October 2025
Seventh Revision Date	16th December 2025