

DOCUMENT CONTROL

Policy Name	Anti-Money Laundering & KYC Policy
Version Number	4
Created by	Risk Analyst
Reviewed by	Head - Risk
Approved by	Board of Directors
Effective From	February 22, 2019
Ownership	Risk Department

Version	Description (First Release/Revision/No Change)	Created by	Reviewed by	Approved by	Date of Board Approval
1	First Release	Head Risk & Credit	Chief Executive Officer	Board of Directors	22 Feb 2019
2	Revision	Head Risk & Credit	Chief Executive Officer	Board of Directors	20 Mar 2025
3	Revision	Head Risk & Credit	Chief Executive Officer	Board of Directors	20 Mar 2026
4	Revision	Risk Analyst	Head - Risk	Board of Directors	July 22, 2026

Statement of Confidentiality

This document is confidential in nature and contains information that is proprietary and confidential to Satin Finserv Limited (SFL) which shall not be disclosed outside SFL, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of Satin Finserv Limited is prohibited.

CHANGES MADE IN THE CURRENT VERSION SINCE THE LAST APPROVED POLICY

Sl. No	Change	Section	Reference Page No
1.	- Added risk categorization for Prime and Secured Assets (PSA) vertical; and - Deleted the clause related to categorization of customer with close family shareholding and B.O. to be classified as high risk.	Client Acceptance Policy	9

TABLE OF CONTENT

Contents

1. Background:	4
2. Money Laundering	4
3. Policy of Satin Finserv Limited.....	5
4. Group- wide AML/CFT Framework.	6
5. Wire Transfer AML Requirements.....	6
6. Money Laundering and Terrorist Financial Risk Assessment.....	7
7. Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standard (CRS)	8
8. Client Acceptance Policy.....	8
9. Client Identification Procedure:.....	11
10. Unique Customer Identification Code (UCIC).....	13
11. Hiring of Employees and Employee Training	13
12. Compliance with the Provisions of Foreign Contribution (Regulation) Act, 2010 –	13
13. Shell Banks –	13
14. Operation of Bank Accounts & Money Mules –	14
15. Risk Management.....	14
16. Suspicious Transaction Reports (STR).....	14
17. Records Management:	15
18. Information to be Preserved	15

1. Background:

This policy is framed in accordance with:

- RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended up to June 12, 2025
- Prevention of Money Laundering Act, 2002 as amended from time to time
- Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 as amended from time to time
- Financial Action Task Force Recommendations
- United Nations Security Council Resolutions
- Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

These directions are issued by Department of Regulation (DoR), Reserve Bank of India

Definitions (Key):

- **Beneficial Owner (BO)**
 - **Company:** >10% of the shares or capital or profits of the company.
 - **Partnership Firm:** >10% of capital or profits of the partnership.
 - **Unincorporated association or body of individuals:** >15% of the property or capital or profits of the unincorporated association or body of individuals.
 - **Trust:** ≥10% interest.
 - Controls through other means included.
- **Politically Exposed Person (PEP)** – Domestic and Foreign
- **V-CIP** – Video based Customer Identification Process
- **CKYCR** – Central KYC Records Registry
- **Money Mule** – Individual allowing misuse of account for illicit flows
- **Designated Director** – Board Level AML oversight
- **Principal Officer** – Financial Intelligence Unit (FIU)– India reporting Authority

2. Money Laundering

Money laundering can be defined as engaging in financial transactions that involves income derived from criminal activity, transactions designed to conceal the true origin of criminally derived proceeds that appear to have been received through legitimate sources/origins. The money laundering activities as defined under Section 3 of The Prevention of Money-Laundering Act, 2002.

Prevention of Money Laundering Act, 2002

Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the rules notified there under came into force with effect from July 1, 2005. The PMLA 2002 and rules notified there under impose an obligation on intermediaries to verify identity of clients, maintain records and furnish information to the Financial Intelligence Unit (FIU)-INDIA.

Financial Intelligence Unit (FIU)-India

The Government of India set up Financial Intelligence Unit-India (FIU-IND) on November 18, 2004 as

an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND coordinates with national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes. It works closely with the Economic Intelligence Council (EIC).

3. Policy of Satin Finserv Limited

SFL shall establish robust measures to prevent money laundering and implement a framework for reporting cash and suspicious transactions to FIU-IND under PMLA 2002, ensuring adherence to updated RBI guidelines:

- No account is opened in anonyms or fictitious/ benami name(s). The onus to ensure this lies with the Branch Manager.
- Periodic KYC updation through multiple channels (branch, BC, digital, V-CIP, Aadhaar OTP where permitted).
- Mandatory use of CKYCR as the primary reference for KYC records at onboarding and during updates.
- KYC records of customers shall be uploaded to the Central KYC Records Registry (CKYCR) within 10 days of opening an account or establishing a business relationship.
- Video-based Customer Identification Process (V-CIP) to be treated as equivalent to face-to-face verification.
- Provision of financing exclusively for legally verifiable business activities, excluding those on the Exclusion List or prohibited by RBI/GoI, and only to bona fide clients for genuine business needs.
- Onboard customers on merit irrespective of caste, creed, religion or gender.
- Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, UN Security Council List of Prohibited clients and other list as may be specified. Further SFL will ensure that the name of the proposed clients is not appearing in the consolidated list of individual and entities circulated by RBI for such purposes and also available at below links:
<https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>
www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
<https://www.un.org/securitycouncil/sanctions/1988/materials>
Any other list as may be specified from time to time.
- SFL shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer
- SFL shall ensure strict compliance with the 'Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005,' as prescribed under Section 12A of the WMD Act, 2005, pursuant to the Order dated January 30, 2023, issued by the Ministry of Finance, Government of India (refer Annex III of the Master Direction on KYC).
- In accordance with paragraph 3 of the aforementioned Order, SFL will ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
- SFL principally does not establish any business relationship with PEPs but it shall have the option of establishing a relationship with PEPs (whether as customer or beneficial

owner) provided that apart from performing normal customer due diligence:

- a. Have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP.
 - b. Sufficient information including information about the sources of funds/wealth accounts of family members and close relatives is gathered on the PEP;
 - c. The identity of the person shall have been verified before accepting the PEP as a customer;
 - d. The decision to open an account for a PEP is taken at a senior level in accordance with SFL's Customer Acceptance Policy;
 - e. All such accounts are subjected to enhanced monitoring on an on-going basis;
 - f. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
 - g. The Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable
 - h. These instructions shall also be applicable to accounts where a PEP is the beneficial owner, their family members or close associates.
- Prior to launch or adoption of any new products, services, delivery mechanisms, or technologies, the Company shall conduct and document an ML/TF Risk Assessment and implement appropriate mitigation measures.

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

4. Group- wide AML/CFT Framework.

Satin Finserv Limited (SFL), a wholly owned subsidiary of SCNL, operates within a Group-wide AML/CFT framework aligned with RBI KYC Directions while retaining full regulatory responsibility. The SCNL Board-approved policy establishes uniform standards for risk management, CDD/EDD, transaction monitoring, sanctions screening, and risk escalation.

Controlled information sharing across the Group on high-risk customers, PEPs, sanctions, and ML/TF typologies is permitted with strict data protection and no tipping-off.

SFL independently manages customer onboarding, monitoring, and regulatory reporting (CTR/STR to FIU-IND) with full confidentiality.

5. Wire Transfer AML Requirements

SFL shall comply with RBI prescribed AML requirements relating to wire transfers, including domestic and cross border transactions.

Key Requirements:

- All cross border wire transfers and domestic wire transfers of ₹50,000 and above shall include:
 - Name of the originator
 - Originator account number (or unique transaction reference)
 - Originator address or officially recognized identification

- Name of the beneficiary
- Beneficiary account number
- SFL shall ensure complete originator and beneficiary information accompanies wire transfers and is retained throughout the payment chain.

Wire transfers with incomplete information or suspicious characteristics shall be subject to Enhanced Due Diligence and reported as Suspicious Transaction Reports (STRs), where applicable

6. Money Laundering and Terrorist Financial Risk Assessment

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

Enterprise-wide ML/TF risk assessment to be carried out at least annually with documented approval by the Risk Management Committee. Interim reviews may be done based on material changes in products, geographies, or regulations.

6.1 Implementation of this Policy: -

Principal Officer of the Company will be responsible for:

- Compliance with the provisions of the PMLA and AML Guidelines.
- Act as a central reference point and play an active role in identification & assessment of potentially suspicious transactions.
- Ensure that SFL discharges its legal obligation to report suspicious transactions to the concerned authorities.
- The Principal Officer (PO) shall monitor electronic update notifications from the CERSAI CKYC Portal. Upon notification, the PO must promptly retrieve updated records via API or SFTP and synchronize them with internal customer profiles to ensure data parity without requiring redundant documentation from the customer.
- Accounts opened via Aadhaar-OTP are considered "Limited Accounts." Under the latest RBI Master Directions, these must be converted to full-status accounts within one year via full CDD. For all such accounts initiated via Aadhaar-OTP, e-KYC, the PO must ensure a transition to full CDD status (prioritizing V-CIP or physical verification) within a strict 12-month statutory window.
- SFL shall ensure that its V-CIP systems are hosted in secure infrastructure located in India.
- It ensures that its V-CIP systems undergo periodic Vulnerability Assessment, Penetration Testing, and CERT in empaneled audits.
- Detected or attempted identity frauds through V CIP shall be documented and reported as required under applicable cyber security and AML regulations.

The main aspect of this policy is to have Client Due Diligence Process which means:

- Obtaining sufficient information about the client in order to identify who is the actual beneficial owner or on whose behalf the transaction is conducted.
- Verify the Client's identity using reliable, independent source document, data or information.
- Conduct on-going due diligence and scrutiny of the account/client to ensure that the

transaction conducted is consistent with the client's background/financial status, activities and risk profile.

The Client Due Diligence Process includes four specific parameters:

- Client Acceptance Policy,
- Client Identification Procedure
- Suspicious Transaction Identification & Reporting
- Monitoring of Transactions

7. Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standard (CRS)

SFL is aware of the regulatory framework under the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS), which apply to Reporting Financial Institutions as defined under the Income-tax Act, 1961 and relevant Rules.

At present, FATCA/CRS obligations are not applicable to SFL, as SFL does not fall under the definition of a Reporting Financial Institution. However, SFL shall:

- Periodically review its business activities and product lines to assess whether it becomes subject to FATCA/CRS requirements in the future;
- Monitor regulatory updates issued by CBDT, RBI, and other competent authorities relating to FATCA/CRS;
- Ensure that necessary systems, controls, and governance mechanisms can be implemented promptly should SFL become subject to FATCA/CRS obligations;
- Escalate any change in applicability to the Designated Director and the Board, and initiate appropriate registration and reporting processes as required.

SFL remains committed to adhering to all applicable statutory and regulatory requirements and shall update this policy accordingly if FATCA/CRS obligations become applicable in the future.

8. Client Acceptance Policy

- a.) Customers may be on-boarded through Face-to-Face (F2F), Aadhaar OTP E/O-KYC (CDD within one year), Video-based Customer Identification Process (V-CIP, equivalent to F2F), Digi-Locker/e-documents, or other digital channels permitted by RBI.
- b.) **Clients on whom we are able to apply appropriate KYC procedures are acceptable:** Obtain complete information from the client. It should be ensured that the initial forms taken by the client are filled in completely; all photocopies submitted by the client are checked against original documents without any exception. Ensure that the 'Know Your Client' guidelines are followed without any exception. All supporting documents as specified by Reserve Bank of India (RBI) are obtained and verified.
- c.) **Clients with identity matching that of persons known to have criminal background are not acceptable:** Check whether the client's identity matches with any person known to have a criminal background or is banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory body worldwide.
- d.) Enhanced Due Diligence (EDD) shall be applied to higher-risk clients including PEPs, NRIs,

NGOs, trusts, companies with opaque ownership, non-face-to-face clients, and clients from high-risk jurisdictions as notified by RBI/FATF/UNSC/MEA. Screening against updated sanction lists is mandatory.

- e.) **Client registration forms which are suspected to be fictitious are not acceptable:** Ensure that no loan is being given in a fictitious/benami name or on an anonymous basis.
- f.) **Submission of mandatory information/documents should not be compromised:** Client's account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Accounts should not be opened where the client refuses to provide information/documents without satisfactory justification.
- g.) **All the Clients would be classified under three categories viz. Low Risk, Medium Risk and High Risk:**

Risk Categorization in Micro Enterprise Group (MEG) vertical and Business Advance Plus product:

Segment	High Risk	Medium Risk	Low Risk
Self-Employed	• All Clients with sales turnover of more than INR 1000 million • All cases of Politically exposed Persons (PEPs) • NRI shareholding of more than 15% as per constitution	• All Clients with sales turnover of more than INR 500 million and less than INR 1000 million.	• All other accounts not classified as High or Medium risk
Salaried	• All cases of politically exposed Persons (PEPs)	• Nil	• All other accounts not classified as High or Medium risk

Risk Categorization in Sustainable & Emerging Businesses (SEB) vertical:

Risk Category	Customer Profile
Low Risk	Borrowers operating in transparent and regulated sectors with clean financial histories and straightforward ownership structures.
Medium Risk	Borrowers in cash-intensive, seasonal, or moderately regulated sectors with some complexity in structure or revenue flows.
High Risk	Borrowers from high-risk sectors or unregulated/complex entities, difficult to verify ownership or source of funds along with NPOs, foreign nationals, politically exposed persons (PEPs), high cash turnover clients.

Risk Categorization in Prime and Secured Assets (PSA) vertical:

Risk Category	Customer Profile
Low Risk	Customers with transparent ownership structures, satisfactory KYC and credit history, identifiable source of funds, stable business operations, clear and marketable collateral title (where applicable), and purchase of standard machinery from verified/empaneled vendors or OEMs.
Medium Risk	Customers with moderate business or ownership complexity, cash-intensive or seasonal businesses, rented or mixed-use collateral, newly established vendor/OEM relationships, non-standard income assessment methods, or cases requiring additional verification of source of income, source of funds, business turnover, end use, or repayment capacity.
High Risk	Customers involving Politically Exposed Persons (PEPs), NRIs, trusts, NGOs, complex beneficial ownership structures, high cash turnover businesses, adverse media findings, machinery refinance, startup machinery finance, refurbished/non-standard machinery funding, special property categories, succession/gift/family-settlement based ownership, or any case requiring Enhanced Due Diligence (EDD) under AML regulations.

High risk clients would also include (a) Non-resident Clients, (b) Trusts, charities, NGOs and organizations receiving donations, (c) Non-face to face Clients and (d) Those with dubious reputation as per public information available etc.

Based on classification defined above, following documents can be additionally accepted for Low-Risk Clients (which are defined as such during the on-boarding stage) as identity or address proof:

- Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks and Public Financial Institutions
- Letter issued by a gazetted officer, with a duly attested photograph of the person.

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

SFL shall issue advance KYC-updation notices through available communication channels, sending at least three reminders at suitable intervals including at least one intimation by physical letter, for complying with the requirement of periodic updation of KYC.

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

- a) Large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

- c) High account turnover is inconsistent with the size of the balance maintained.
- d) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

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

9. Client Identification Procedure:

Documents to be obtained as part of Client identification procedure for new clients:

- **Individuals:** Any one certified copy of the following must be obtained:
 - (i) **Identity Proof:** Any one from the following documents to be considered for Identity proof
 - Aadhaar card issued by UIDAI may be used in masked form; if used for e-KYC, follow UIDAI authentication rules.
 - Voter Identity card
 - Passport
 - PAN is mandatory for certain transactions as per RBI/Income Tax rules
 - Driving License
 - Ration Card
 - Any Government/PSU/Bank issued photo identity card
 - NREGA Job Card or any other document prescribed by the regulatory authorities

If these documents also contain address details, then it would also be accepted as ‘proof of address. If the document submitted for proof of identity does not contain address details, then client will have to submit another officially valid document (OVD) which contains address details.
 - (ii) **Address Proof:** Any one of the following documents to be considered for valid address proof
 - Voter Identity Card
 - Passport
 - Bank Statement
 - Aadhaar
 - Ration card or latest Electricity/telephone bill (of the latest billing cycle) in the name of the client
 - Any other document prescribed by the regulatory authorities.

Address change may be accepted through self-declaration, subject to positive confirmation via digital/branch/BC channels.
- **Companies:** The copy of the following must be obtained for KYC and due diligence purpose:
 - Copy of Registration/Incorporation Certificate
 - Copy Memorandum & Articles of Association
 - Copy of PAN Card and the list of directors along with Director Identification No. (DIN)
 - Copy of shareholding pattern and list of beneficial owners (BO)
 - Copy of latest audited Annual Statements of the corporate client
 - Resolution of Board of Directors to conduct the transactions
 - Copy of latest telephone bill in the name of the company (of the latest billing cycle)
 - Copy of latest electricity bill in the name of the company (of the latest billing cycle).
- **Partnership Firm:** The copy of the following must be obtained (whatever is applicable):

- Registration Certificate, if registered
 - Partnership Deed
 - Certified Pan Card of Partners
 - Power of Attorney granted to a partner or an employee to transact the business on its behalf
 - Any officially valid document identifying the partners and the persons holding the power of attorney and their addresses
 - Copy of latest Telephone Bill in the name of the firm (of the latest billing cycle)
 - Copy of latest electricity bill in the name of the firm (of the latest billing cycle).
- **Trust & Foundations:** The copy of the following must be obtained (whatever is applicable):
 - Registration Certificate, if registered
 - Trust Deed
 - Power of Attorney granted to transact the business on its behalf
 - Any officially valid document (OVD) to identify the trustees, settlers, beneficiaries and those holding Power of Attorney
 - Founders/managers/Directors and their addresses
 - Resolution of managing body of the Foundation/Association
 - Copy of latest Telephone Bill in the name of the trust & foundations (not more than 2 months old)
 - Copy of latest electricity bill in the name of the trust & foundations (not > 2 months old).
 - **Unincorporated association or a body of individuals:** The copy of the following must be obtained, (whatever is applicable):
 - Resolution of the managing body of such association or body of individual
 - Power of Attorney(“POA”) in favor of person authorized to transact
 - Officially valid documents like PAN Card, Voters ID, Passport, etc. to identify the person(s) authorized to transact
 - Any document required by SFL to establish the legal existence of such association or body of individuals.
 - **Proprietary Concern:** Any two of the below documents would suffice. These documents should be in the name of the proprietary concern:
 - Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/license issued by the Municipal authorities under Shop & Establishment Act
 - Income tax/ GST returns and certificate issued by Professional Tax authorities
 - License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.
 - Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department.
 - Importer Exporter Code (IEC) issued to the proprietary concern by the office of Directorate General of Foreign Trade (DGFT) as an identity document for opening of account.
 - 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/acknowledged by the Income Tax Authorities.
 - Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

- **NRI:** One certified copy of the following must be obtained:
 - Copy of the Passport
 - Copy of the PAN Card
 - Proof of Overseas address and Indian address
 - Copy of Bank Statement.

All the client identification documents will be mandatorily verified online or in offline mode.

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

High risk accounts must be subjected to more intensify monitoring. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

10. Unique Customer Identification Code (UCIC)

SFL shall allot a Unique Customer Identification Code (UCIC) to each customer at the time of establishing a business relationship.

- UCIC shall be used to uniquely identify the customer across products, locations, and delivery channels.
- UCIC shall also be assigned to existing customers, where not already allotted.

The UCIC framework shall enable effective monitoring of customer relationships and transactions on a consolidated basis.

11. Hiring of Employees and Employee Training

- i. Adequate screening mechanism including Know Your Employee / Staff policy, as an integral part of the personnel recruitment/hiring process shall be put in place.
- ii. SFL shall endeavor to ensure that the staff dealing with/being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Regulated Entities (RE) shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

12. Compliance with the Provisions of Foreign Contribution (Regulation) Act, 2010 –

Company shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, Company shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank of India based on advice received from the Ministry of Home Affairs, Government of India

13. Shell Banks –

SFL shall not establish or maintain any relationship with shell banks.

14. Operation of Bank Accounts & Money Mules –

Monitoring of accounts and transactions shall be strictly adhered to, in order to minimize the operations of “Money Mules” which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties, which act as “money mules”.

15. Risk Management

The following elements of SFL shall address risks arising from non-compliance with the Prevention of Money Laundering Act (PMLA):

- The Board shall ensure the implementation of an effective KYC program by establishing appropriate procedures and monitoring their effective execution.
- Internal audit and compliance function would evaluate and ensure adherence to the KYC policy and procedures and provide independent evaluation of it, including legal and regulatory requirements. Internal auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be placed before the Audit Committee of the Board on quarterly basis.

Periodic updation of KYC will be required as per the following customer risk category:

- Low risk – every 10 years;
- Medium risk – every 8 years;
- High risk – every 2 years.

Based on the half-yearly review, risk categorization for all borrowers shall be updated in the Loan Management System (LMS) and reported to the CEO. Following the CEO’s review, the Operations Head shall authorize the risk categorization data within the LMS.

Within the context of SFL, loan disbursements shall be executed strictly in accordance with the Credit Policy and established processes, which define the target market, industry segments, and required documentation. Consequently, the entire due diligence and disbursement process is governed under the Credit Policy framework.

With respect to customer-level transactions, particularly collections, any amount received that cannot be clearly and directly attributed to the repayment obligations of the borrower shall be classified as a suspicious transaction and handled in accordance with applicable regulatory and internal guidelines.

For eg.:

- a. Mr. X has been funded Rs. 2 lakhs and current principal outstanding is Rs. 1.80 lakhs. Mr. X wants to foreclose the contract and pays us Rs. 3 lakhs whereas the foreclosure value is Rs. 2.20 lakhs (Rs. 1.80 lakhs + foreclosure charges Rs. 40,000).
- b. Mr. Y has already foreclosed his loan with SFL in the m/o January from his own funds. He again makes a payment which is to the tune of > Rs 50,000 in the subsequent month.

16. Suspicious Transaction Reports (STR)

SFL would be guided by the definition of suspicious transaction as contained in the PMLA and rules made thereunder, as amended from time to time.

The Principal Officer - shall file STR with FIU-IND within 7 working days of determination, in the

prescribed electronic format. STRs must be also filed for attempted transactions. Post-filing, transactions may continue but without tipping-off the customer.

SFL is not empowered to seize any counterfeit currency. However, the following incidents of counterfeit currency at the cash counter would be recorded and repeated occurrence would be reported.

- Bulk counterfeit currency of more than 10 pieces at a time;
- Repeated event within a week from a collection executive or client.

All Cash Transaction Report (CTR)/ Suspicious Transaction Report (STR) would be filed electronically by the 15th of next month or as per the norms stipulated by FIU-IND from time to time.

17. Records Management:

All KYC, V-CIP recordings, consent logs, CKYCR download logs, and Aadhaar authentication logs shall be securely maintained by the company. These records must be retained for a minimum period of 5 years from the date of account closure or completion of the relevant transaction, whichever is later, in accordance with applicable regulatory requirements

The Company shall establish, document, and implement appropriate procedures to ensure the preservation, security, and accessibility of all records related to KYC due diligence, ongoing monitoring, and other anti-money laundering (AML) and counter-terrorist financing (CFT) measures.

For the purpose of record retention, the term “Transaction” shall have the same meaning as defined under Rule 2(h) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2013, i.e., a “transaction” includes a purchase, sale, loan, pledge, gift, transfer, delivery, or any arrangement thereof, and also covers:

- a) Opening of an account;
- b) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- c) Use of a safety deposit box or any other form of safe deposit;
- d) Entering into any fiduciary relationship;
- e) Any payment made or received in whole or in part of any contractual or other legal obligation;
- f) Any payment made in respect of playing games of chance for cash or kind including activities associated with casino.
- g) Establishing or creating a legal person or legal arrangement.

17.1 Transactions for which records must be maintained:

The Company shall retain records pertaining to the following categories of transactions:

- a) All series of cash transactions integrally connected to each other, which have taken place within a month.
- b) 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.
- c) All suspicious transactions whether or not made in cash.

18. Information to be Preserved

The following details must be retained for all transactions: the nature of the transaction, the amount and currency denomination, the transaction date, and the parties involved. A copy of this information shall be duly signed by the individual responsible for the transaction and maintained in a separate file along with all other related documentation.

Independent Assessment: Internal audit shall annually assess compliance with RBI Master Directions, including V-CIP processes, CKYCR retrievals, Aadhaar OTP timelines, STR filing, and KYC pendency MIS. Observations to be placed before the Audit Committee.

An annual independent assessment of the implementation and effectiveness of this policy shall be conducted by the Company's internal auditors as part of their annual review process. Observations and comments regarding adherence to this policy, RBI guidelines, and other applicable statutory requirements shall be presented to the Audit Committee.

To ensure compliance with the obligations under the Act and Rules, Board may appoint/nominate designated director and principal officer required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The details of the Designated Director and Principal Officer are given below:

Designated Director:

Name and Designation	Mr. Pramod Marar, Whole Time Director & CEO
Address	Corporate Office: Plot No. 492, Udyog Vihar, Phase – III, Gurugram, Haryana – 122016, India
Contact details	Email id: secretarial@satinfinserv.com

Principal Officer:

Name and Designation	Mr. Arjun Bansal, Chief Financial Officer
Address	Corporate Office: Plot No. 492, Udyog Vihar, Phase – III, Gurugram, Haryana – 122016, India
Contact details	Email id: secretarial@satinfinserv.com

In case any further information/clarification is required in this regard, the 'Principal Officer' as designated/ nominated maybe contacted.