RAJASHREE TRACOM PRIVATE LIMITED (RTPL)

KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY LAUNDERING POLICY

Version Control		
Version Number	**Description**	**Date**
Version 0.1	New Policy	8th April 2022

Effective Date: 8th April 2022

Next Review Date: 30th September 2022

Policy Owner: Operations Department

Prepared By :

Reviewed by :

Approved By :

Table of Contents

1. Introduction

In accordance with the Master Directions issued (as amended from time to time) by Reserve Bank of India, all Regulated Entities (REs) including Rajashree Tracom Pvt Limited (RTPL) is required to put in place appropriate Policy and procedures to comply with the relevant Know Your Customer (KYC) norms and Customer Due Diligence (CDD) processes at the time of on-boarding the Customer and also during the continued relationship with such Customer which includes monitoring of transactions in terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as well as the relevant norms as put out by RBI.

2. Policy Statement

RTPL is primarily engaged in retail finance and by nature of its business operations, the potential risks of money laundering, terrorist financing that it faces is relatively low. RTPL recognizes the importance of the AML programs and commits itself to inculcating a vigilant culture in combating money laundering to the extent applicable to the firm. Accordingly, it puts in place a detailed KYC & AML Policy and procedures hereunder in line with RBI Directions and Prevention of the Money Laundering Act, 2002/Rules as amended from time to time as well that of the norms put out by the other relevant regulations that is applicable to its business operations, for the time being in force.

3. Objectives of the policy:

The Policy seeks to achieve the following objectives.

- To provide a framework for how the company, in its process of conducting business with Customers, will deal with the threat of money laundering and terrorism financing.
- To prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities
- That all the staff are aware and receive training on the Anti Money laundering legislation
- applicable to them, as well as to adhere to their responsibilities under the regulations
- To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
- To enable the Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities as
- envisaged under the Prevention of Money Laundering Act, 2002 and in accordance with laid down procedures.
- To comply with applicable laws and regulatory guidelines

4. Scope of this Policy

This Policy applies to all employees of RTPL and third-party agents engaged by it for origination, fulfilment, collection, outsourcing agencies, etc. The Policy seeks to maintain high standards of conduct within the Company and among its agents, if any, by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Company to comply with its legal obligations. The legislation and Regulatory directives places responsibility upon RTPL, its employees and its agents to combat money laundering and covers a very wide area of financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime. It applies to all employees involved with handling monetary transactions. It is a criminal offence to, assist a money launderer, “tip off” a person suspected to be involved in money laundering that they are suspected or that they are the subject of police investigations, fail to report a suspicion of money laundering and acquire, use, or possess criminal property. The legislative requirements concerning anti-money laundering procedures are extensive and complex. This Policy aims to meet the legal requirements proportionate to the intensity of risks that RTPL is exposed to in respect of the businesses/activities (business verticals) being undertaken by the company as detailed below.

- Gold Loan including all types (online or offline)
- Unsecured Micro Enterprise loans to MSME
- Secured Loan against property
- Personal Loan to Salaried Employees/Teachers
- Loans to Corporates

5. Key Definitions

1. **Beneficial Owner (BO)**

a) Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
   a. "Controlling ownership interest" means ownership of/entitlement to more
   b. than 25 per cent of the shares or capital or profits of the company.
   c. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or
   d. voting agreements.

b) Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

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

2. **"Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

3. **"Designated Director"** means a person designated by the RE (RTPL) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors,
Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

4. **"Customer"** means.
   a. a person or entity that maintains and/or has a business relationship with the Company;
   b. one on whose behalf such relationship is maintained (i.e. the beneficial owner);
   c. any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company;

5. **"Digital KYC"** means capturing live photo of the Customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Regulated Entity (RE) as per the provisions contained in the Act.

6. **"Digital Signature"** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

7. "**Equivalent e-document"** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the Customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

8. **"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.

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

10. **"Non-face-to-face Customers"** means Customers who open accounts without visiting branches /offices of RTPL or meeting its officials.

11. **"Obtaining certified copy of Officially Valid Document (OVD)"** – Means comparing the copy of OVD with the original and recording the same on the copy by authorized officer of RTPL. Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

    - authorised officials of overseas branches of Scheduled Commercial Banks registered in India, branches of overseas banks with whom Indian banks have relationships,
    - Notary Public abroad,
    - Court Magistrate, Judge,
    - Indian Embassy/ Consulate General in the country where the non-resident Customer resides.

12. "**Offline verification"** means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as per clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

13. **"Senior Management"** Senior Management for the purpose of the Policy shall constitute MD & CEO, CS, CFO, CTO Head- Credit, Head – Operations, Head- Compliance and Head- Risk Management.

14. **"Video based Customer Identification Process (V-CIP)"**: a method of Customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual Interaction with the Customer to obtain identification information including the documents required for Customer Due Diligence (CDD) purpose, and to ascertain the veracity of the information furnished by the Customer. Such process shall be treated as face-to-face process.

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

6. Key elements 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. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The Company had framed its KYC policy incorporating the following four key elements:

I. Customer Acceptance Policy
II. Customer Identification Procedures
III. Monitoring of Transactions; and
IV. Risk management.

6.1. Customer Acceptance Policy (CAP)

RTPL's CAP lays down criteria for acceptance of Customers. While taking decision to grant any facilities to the Customers as well as during the continuation of any facilities the following norms and procedures will be followed by the company

a) No account will be opened in anonymous or fictitious/benami name.
b) Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done 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.
c) RTPL will refrain from opening an account where the company is unable to apply appropriate Customer Due Diligence (CDD) measures either due to non-cooperation of the Customer or non-reliability of the documents/information furnished by the Customer.

d) A Unique Customer Identification Code (UCIC) shall be allotted to new and existing Customers. RTPL shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant Customer of RTPL desires to open another account with RTPL, there shall be no need for a fresh CDD exercise.
e) Suitable system is put in place to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
f) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
g) Where an equivalent e-document is obtained from the Customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

Implementation of CAP should not become too restrictive and result in denial of the RTPL's services to public, especially those who are financially or socially disadvantaged.

6.2. Customer Identification Procedure (CIP)

The policy approved by the Board of the Company clearly spells out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant Guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to the Company and a burdensome regime for the customers.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc).

- For customers that are natural persons, the Company will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.
- For customers that are legal persons or entities, the Company will (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure-I for guidance of the Company.

6.3. Customer Due Diligence Procedure (CDD) in case of Individuals

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lender's prudence and the legal requirements as per established practices. The Company will take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

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

- A certified copy of Officially Valid Documents (OVD), as given in Annexure I.
- One recent photograph (For the gold loan Customers capturing of photos of the individuals and keeping in the ERP to be continued).
- Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and such other documents pertaining to the nature of business or financial status specified in this Policy.

6.3.1. Offline verification through proof of possession of AADHAAR number:

RTPL may carry out Offline Verification of Customers if they are desirous of undergoing AADHAAR Offline Verification for identification purposes. No such offline verification shall be performed without obtaining the written consent of the Customer in the manner prescribed in the AADHAAR Regulations.

Wherever AADHAAR details are collected, it shall be ensured that Customers have redacted or blacked out their AADHAAR numbers through appropriate means. The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification, when NBFCs or itself are authorised by RBI to do such verification for establishing account-based relationship.

6.3.2. Verification of equivalent E-Document:

Where the Customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the Customer, RTPL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the Customer as specified in the guidelines for digital KYC.

6.4. Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to verify his/her identity shall be undertaken keeping in view the following:

a.) Where the Customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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

6.5. CDD measures in respect of non-individuals:

CDD Standards and documents to be collected in respect of Proprietary firms, partnership firms, companies and other Legal entities are given in Annexure I.

7. Customer Due-Diligence by Third Party

In compliance of the KYC regulations, RTPL may rely on the Customer due diligence done by third parties, for verifying identity of Customers at the time of commencement of account-based relationship, subject to the following conditions.

a) Records or information of the Customer due diligence carried out by the third party is obtained within 2 days from the third party or from Central KYC Records Registry.

b) RTPL is satisfied that copies of the identification data and other relevant documents relating to the Customer due diligence requirements will be available from the third party upon request without delay.

c) The third party is regulated, supervised, or monitored and has capabilities to comply with the Customer due diligence and record keeping requirements as prescribed in the Prevention of Money Laundering Act.

d) The third party shall not be based in a country or jurisdiction assessed as high risk.

The ultimate responsibility for Customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with RTPL. (Description of RE are given in Annexure II).

8. Simplified Procedures for small value loans

For Customers with aggregate loans below Rs.0.50 lakh, Proof of Identity alone will be sufficient provided that the Customer gives full and complete address in the loan application form and his telephone number is confirmed by the branches to be correct. If a person is unable to produce identity documents as mentioned in Annexure I (i.e., any of OVDs and PAN/ Form 60), interim / Temporary KYC documents such as Labour card, Civil ID card, Credit Card, Employer Company ID card, LIC card, State ID card, Bank Pass Book, etc. may be accepted subject to the following conditions:

a) The Customer shall provide his self-attested photograph.

b) Branch Head/ Designated Officer of RTPL shall certify under his/her signature that the Customer has affixed his signature or thumb impression in his presence.
c) The account shall remain operational initially for 12 months, within which the Customer must furnish his identity documents for conducting CDD as mentioned in para 6.3. Customer shall be suitably informed at the time of starting the relationship.
d) Maximum outstanding shall not exceed Rs 0.50 Lakh in all their accounts taken together at any point of time and the total credit in all the accounts taken together shall not exceed Rs. 1.00 lakh in a year.
e) The Customer shall be made aware that no further transaction will be permitted until full KYC procedure is completed in case of condition no. d. as mentioned above is breached.
f) Regularization of Interim/Temporary KYC: In-order to avoid any inconvenience to the Customers RTPL shall notify the Customer when the balance reaches rupees forty thousand (Rs. 40,000/-) or the total credit in a year reaches rupees eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted and that otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds Rs 0.50 Lakh at any point of time or the total credit in the accounts in year exceeds Rs 1.00 Lakh.

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

9. Selling Third party products

While selling third party products, RTPL shall comply with the following directions:

a) Identity and address of the walk-in Customers shall be verified for transactions above Rs 0.50 lakh, whether conducted as a single transaction or several transactions that appear to be connected.
b) Transaction details of sale of third-party products and related records shall be maintained as specified under this Policy.
c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with Customers including walk-in Customers shall be made available.
d) Transactions involving Rs 0.50 lakh and above shall be undertaken only by:
    a. Debit to Customer's account or against cheque, transfer from banks / debit cards / credit card etc.
    b. Obtaining and verifying PAN (regular Customer as well as walk in Customer).

10. Monitoring of Transactions

RTPL shall monitor transactions on an ongoing basis for the purpose of reporting it to the appropriate authorities in case any suspicious transactions are found to be carried out by the concerned Customer. (An illustrative list of suspicious transactions is given in Annexure III).

The extent of monitoring by the RTPL will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose.

RTPL shall exercise caution with respect to the transactions with persons (including legal persons and other financial institutions) from the countries which have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF Recommendations, 2012.

RTPL shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling under FATCA in terms of the direction of the RBI/PMLA in respect of all products/ services.

11. On-going Due Diligence

a) RTPL shall undertake on going due diligence of Customers to ensure that their transactions are consistent with their knowledge about the Customers, Customers' business and risk profile; and source of funds.
b) Without prejudice to the generality of factors that call for close monitoring, the following types of transactions are monitored closely:
    a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the Customer, which have no apparent economic rationale or legitimate purpose.
    b. Transactions which exceed the thresholds prescribed for specific categories of accounts.

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

c) The extent of monitoring shall be aligned with the risk category of the Customer and high-risk category accounts shall be subjected to more intensified monitoring.
d) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

12. Periodic Updation

Periodic updation shall be carried out at least once in every two years, for high risk Customers, once in every eight years for medium risk Customers and once in every ten years for low risk. Customers as per the following procedure:

a) For Individual Customers
- No change in KYC information: In case of no change in the KYC information, a self-declaration from the Customer in this regard shall be obtained through Customer's email-id registered with the RTPL, Customer's mobile number registered with the RTPL, digital channels (such as mobile application of RTPL), letter etc.
- Change in address: In case of a change only in the address details of the Customer, a self-declaration of the new address shall be obtained from the Customer through Customer's email-id registered with the RTPL, Customer's mobile number registered with the RTPL, digital channels (such as mobile application of RTPL), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
- Further, RTPL, may at its option, obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as mentioned in Annexure 1, for the purpose of proof of address, declared by the Customer at the time of periodic updation.

b) Customers other than Individuals
- No change in KYC information: In case of no change in the KYC information of the LE (Legal Entity) Customer, a self-declaration in this regard shall be obtained from the LE Customer through its email id registered with RTPL, digital channels (such as mobile application of RTPL), letter from an official authorized by the LE in this regard, board resolution etc.
- Further, RTPL shall during this process ensure that the Beneficial Ownership (BO) information available is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- Change in KYC information: In case of change in KYC information, RTPL shall undertake the KYC process equivalent to that applicable for on-boarding a new LE Customer.

c) Additional Measures- In addition to the above, RTPL shall also ensure that,
- The KYC documents of the Customer as per the current CDD standards is available and this shall be applicable even if there is no change in Customer information but the documents available with the RTPL are not as per the existing CDD standards. Further, in case the validity of the CDD documents available with RTPL has expired at the time of periodic updation of KYC, RTPL shall undertake the KYC process equivalent to that applicable for on-boarding a new Customer.
- Customer's PAN details, if available with the RTPL, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- An acknowledgment is provided to the Customer mentioning the date of receipt of the relevant document(s), including self-declaration from the Customer, for carrying out periodic updation.
- In order to ensure Customer convenience, RTPL may consider making available the facility of periodic updation of KYC at any of its branches.
- RTPL shall adopt a risk-based approach with respect to periodic updation of KYC.

(Note: The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.)

13. Existing Customers

In case of existing Customers, RTPL shall obtain PAN or Form No.60 by such date notified by the Central Government, falling which RTPL shall temporarily cease operations in the account till the time the PAN number or Form No.60 is submitted by the customer.

Prior to ceasing operations of an account temporarily, RTPL shall give the clients an accessible notice and reasonable opportunity to be heard. RTPL may allow relaxations for continued operations of the account, if the borrower is unable to provide these documents due to injury, infirmity on account of old age or otherwise etc for a maximum period of 6 months. These relaxations shall be permitted by Senior Management.

For gold loan Customers, a copy of the PAN Card of the borrower shall be collected for all transaction above 5 lakh as guided by the regulatory guidelines to NBFCs financing against the collateral of gold.

14. Risk Management

RTPL has put in place appropriate procedures to ensure effective implementation of KYC guidelines.

a) Risk categorization of Customers shall be undertaken based on various factors, such as Customer's identity, nature of employment, business activity of the Customer, location of Customer and his/its clients, mode of payments, volume of turnover, social / financial status and credit history
b) RTPL has categorized its Customers into 'High Risk / Medium Risk / Low Risk' based on the profile of the Customers. RTPL shall apply higher due diligence measures keeping in view the risk level
c) RTPL has developed robust underwriting procedures for on boarding borrowers, which include verification of ownership of the gold ornaments (in the case of gold loans), assessment of financial resources of the borrowers, collection of their market reports etc (for other loans).
d) RTPL's internal audit periodically evaluates the level of adherence to the KYC procedures.
e) Audit function shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

15. Money Laundering and Terrorist Financing Risk Assessment

RTPL 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

The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, cognizance of the overall sector-specific vulnerabilities if any, that the regulator/supervisor may share from time to time shall be taken.

The risk assessment exercise shall be conducted on a quarterly basis and parameters of the assessment shall be modified, in alignment with the outcome of the risk assessment exercise. An internal document detailing the assessment process may be kept separately for the same. The outcome of the exercise shall be put up to Board and should be available to competent authorities and self-regulating bodies.

16. Enhanced Due Diligence

Accounts of Politically Exposed Persons (PEP): Politically Exposed Persons are those individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

Special care and diligence will be taken in respect of Politically Exposed Persons. Generally, the RTPL may not (would not) open accounts of PEP. However, any request from PEPs shall be escalated to Senior management and will be dealt with based on their approval and will be subject to enhanced due diligence (comprising of additional documents) and monitoring.

In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is to be obtained to continue the business relationship. In any case, it must be ensured that sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP.

Accounts of Non-Face-To-Face Customers: These Customers are those who opened accounts without visiting the branches / offices of RTPL or meeting its officials. RTPL shall ensure that first payment from these accounts shall be affected through the Customers' KYC-Complied account with another Regulated Entity.

17. Confidentiality of Information about Customers

All the information collected from the Customers by RTPL shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the Customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that behalf.

Information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Exception to the confidentiality of customer information shall be as under:

- Where disclosure is under compulsion of law.
- Where there is a duty to the public to disclose.
- The interest of the company requires disclosure.
- Where the disclosure is made with express or implied consent of the customer. [KYCs will be shared with DA or co lending partner]

18. Maintenance of Records of Transactions

RTPL take all reasonable steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules thereunder. RTPL shall

a) maintain all necessary records of transactions between RTPL and the customer, both domestic and international, for at least five years from the date of transaction or any other higher periods specified in any other law

b) preserve the records pertaining to the identification of the Customers and their addresses obtained while opening the account and during business relationship, for at least five years after the business relationship is ended.

c) Make available the identification records and transaction data to the competent authorities upon request;

d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005) maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit reconstruction of individual transaction, including the following:
    - 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; and
    - the parties to the transaction.

e) RTPL have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

f) maintain records of the identity and address of its Customers, and records in respect of transactions referred to in Rule 3 of PML Rules, in hard or soft format.

19. Customer Education

Implementation of KYC procedures requires the Company to demand certain information from customers which may be of personal nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company will prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC policy. The front desk staffs will be specially trained to handle such situations while dealing with customers.

20. Appointment of Compliance Officer

The Company to appoint a senior management officer to be designated as Compliance Officer. Compliance Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He/ She shall maintain close liaison with enforcement agencies, banks and any other institutions, which are involved in the fight against money laundering and combating financing of terrorism.

21. Deviations

No deviations or exemptions shall normally be permitted in the documents specified. In case of any extreme cases of exceptions, concurrence of Policy section should be obtained duly recording the reasons for the same. Suitable

operating Guidelines for implementation of the KYC/ AML Guidelines shall be issued and amended for its different business segments from time to time.

Annexure – I KYC Documentation

Details	KYC Documents
Photograph	2 passport size photographs of applicant, preferably, along with spouse combined, The photograph should be signed across on the front. In case of single woman, only client's photograph should be affixed and cross signed/thumb impressed by the client.
Identify Proof	1. Aadhaar card **(Mandatory)** 2. Voter Identity Card **(Most preferred)** 3. Passport 4. PAN card [Mandatory if Loan amount is more than 5Lacs] 5. Driving License 6. Job Card issued by NREGA duly signed by an officer of the State Government 7. Identity card (subject to the Company's satisfaction) / Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company
Address proof	1. Aadhaar card **(Mandatory)** 2. Voter Identity Card **(Most preferred)** 3. Ration card 4. Driving License 5. Passport 6. Letter from any recognized public authority 7. Electricity bill [Not later than previous month] 8. Telephone bill [Not later than previous month] 9. Bank account statement [Not later than previous month] 10. Letter from employer (subject to satisfaction of the Company) 11. A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority. Any one document which provides customer information to the satisfaction of the company will suffice

Annexure II: Regulated Entities:

a) All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949.
b) All India Financial Institutions (AIFIs).
    a. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).
    b. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
    c. All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
c) Depository Participant (DP) services.

Annexure III: Illustrative List of Suspicious Transactions

Broad categories of reasons for suspicion and examples of suspicious transactions generally observed in Non-Banking Financial Companies are indicated as under:

1. IDENTITY OF CLIENT:
   - False identification documents
   - Identification documents which could not be verified within reasonable time
   - Accounts opened with names very close to other established business entities.
2. BACKGROUND OF CLIENT:
   Suspicious background or links with known criminals.
3. MULTIPLE ACCOUNTS:
   Large number of accounts having a common account holder, introducer, or authorized personnel.
4. SIGNATORY WITH NO RATIONALE:
   a) Unexplained transfers between multiple accounts with no rationale.
5. ACTIVITY IN ACCOUNTS:
   - Unusual activity compared with past transactions- Sudden activity in dormant accounts;
   - Activity inconsistent with what would be expected from declared business.
6. NATURE OF TRANSACTIONS:
   - Unusual or unjustified complexity.
   - No economic rationale or bonafide purpose.
   - Frequent cash transactions.
   - Nature of transactions inconsistent with what would be expected from declared business.
7. VALUE OF TRANSACTIONS:
   - Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
   - Value inconsistent with the client's apparent financial standing.
8. INDICATORS OF SUSPICIOUS TRANSACTIONS:
   - Reluctant to part with information, data, and documents.
   - Submission of false documents, purpose of loan and detail of accounts.
   - Reluctance to furnish details of source of funds.
   - Reluctance to meet in person, representing through power of attorney.
   - Approaching a distant branch away from own address.
   - Maintaining multiple accounts without explanation.
   - Payment of initial contribution through unrelated third-party account.
   - Suggesting dubious means for sanction of loan.
   - Where transactions do not make economic sense.
   - Where doubt about beneficial ownership.
   - Encashment of loan through a fictitious bank account.
   - Sale consideration quoted higher or lower than prevailing prices.
   - Request for payment in favor of third party with no relation to transaction.
   - Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent.
   - Frequent request for change of address.
   - Over-payment of instalments with a request to refund the overpaid amount.

Annexure IV: Digital KYC Process (RBI Guidelines)

A. The RE shall develop an application for digital KYC process which shall be made available at Customer touch points for undertaking KYC of their Customers and the KYC process shall be undertaken only through this authenticated application of the REs.
B. The access of the Application shall be controlled by the REs and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by REs to its authorized officials.
C. The Customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the Customer.
D. The RE must ensure that the Live photograph of the Customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system
E. Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the Customer.
F. The Application of the RE shall have the feature that only live photograph of the Customer is captured
G. and no printed or video-graphed photograph of the Customer is captured. The background behind the Customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the Customer.
H. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and watermarking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
I. The live photograph of the Customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
J. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the Customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
K. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to Customer's own mobile number. Upon successful validation of the OTP, it will be treated as Customer signature on CAF. However, if the Customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.
L. In any case, the mobile number of authorized officer registered with the RE shall not be used for Customer signature. The RE must check that the mobile number used in Customer signature shall not be the mobile number of the authorized officer.
M. The authorized officer shall provide a declaration about the capturing of the live photograph of Customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
N. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to Customer for future reference.
O. The authorized officer of the RE shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the Customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including