Policy On
'Know Your Customer' Guidelines
And
'Anti-Money Laundering' Standards

RAPIPAY FINTECH PRIVATE LIMITED

Document Version	Effective Date	Owned By	Approved By
V 2.1	11th November 2019	Head || IT	Board
V 2.2	25th January 2020	Head || IT	Board
V 2.3	31st August 2020	Head || IT	Board
V 2.4	10th February 2021	CTO	Board
V 2.5	9th August 2021	CTO	Board
V 2.6	4th February 2022	IT	Board
V 2.7	26th April 2022	IT	Board
V 2.8	5th August 2022	IT	Board

Table of Contents

Introduction

The Reserve Bank of India ("RBI") has issued Master Direction on Issuance and Operation of Prepaid Payment Instruments ("Direction") which governs the functioning of the companies issuing prepaid payment instruments ("PPI"). Among other things contained in the Direction, RBI requires adoption of 'Know Your Customer' ("KYC") guidelines - Anti Money Laundering (AML), as defined in the PML Act (*defined hereinafter*), thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers from time to time, by the entities issuing PPI and their agents. These guidelines incorporate the recommendations made by the Financial Action Task Force on anti-money laundering standards and combating financing of terrorism as these are being used as the International Benchmark for framing the stated policies, by the regulatory authorities.

In view of the same, **Rapipay Fintech Private Limited** *(Formerly known as Virgosoft IT Services Private Limited)* ("Company" or "RFPL") has adopted a robust policy frame work on KYC and AML measures in line with the prescribed RBI guidelines ("KYC-AML Policy" or this "Policy"). The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications to the Policy, if necessary, to conform to the standards so prescribed. The contents of the Policy shall always be read in tandem/auto- corrected with the changes/modifications which shall be advised by RBI from time to time.

Objective:

The objective of the Policy 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 (*defined hereinafter*) and its financial dealings better which in turn will help it to manage its risks prudently.

Senior Management includes Directors of the Company. Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures as applicable to Company are implemented effectively.

This Policy includes 7 (seven) key elements:

I) Customer Acceptance Policy ("CAP");
II) Customer Identification Procedures ("CIP");
III) Monitoring of Transactions;
IV) Risk Management.
V) Customer Grievance/Dispute Management
VI) PPI Interoperability Policies
VII) Reporting to Financial Intelligence Unit – India

Applicability:

It may be noted that this Policy as stated in this document shall prevail over anything else contained in any other document, process, circular and / or instruction that has been issued by RFPL in this regard and shall be applicable to all verticals and products of the Company, whether existing or rolled out in future.

Definitions:

In this Policy, unless there is anything in the subject or context inconsistent therewith, the expressions listed below shall, when capitalized, have the following meanings:

1. **"Agents"** shall mean the any person appointed by the Company or by the Agents representing the Company, for furthering the business objects of the Company.
2. **"AML"** stands for anti-money laundering.
3. **"Beneficial Owner"** shall mean the ultimate natural person who *inter alia* fulfills the criteria provided in Sub Clause 8 of Part II (*Customer Identification Procedures*) of this Policy.
4. **"CDD" or Customer Due Diligence** shall mean the process of the identifying and verifying the Customers and the Beneficial Owners.
5. **"Central KYC Records Registry"** shall mean an entity defined under Rule 2(1)(aa) of the PML Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a Customer.
6. **"CFT"** stands for combating financing of terrorism.
7. **"Customer"** shall mean any Person that (a) has a business relationship with the Company and/or its Agents;(b) has a financial transaction or activity with the Company and / or its Agents; (c) is connected with a financial transaction which can pose significant reputation or other risks to Company.The definition of "Customer" shall include any Person who is in process of or is proposing to become a customer of the Company.
8. **"KYC"** stands for know your customer.
9. **"Master Directions"** shall have the meaning given to such term in the Introduction to this Policy.
10. **"Person"** includes an individual, statutory corporation, company, body corporate, partnership, joint venture, association of persons, Hindu Undivided Family (HUF), societies (including co-operative societies), trust, unincorporated organization and other bodies / agencies as may be considered as "Person" by RFPL.
11. **"PEP"** shall mean a politically exposed person.
12. **"PMLA Act"** shall mean the Prevention of Money Laundering Act, 2002, including all the rules / regulations made pursuant thereto, as amended from time to time
13. **"PML Rules"** shall mean Prevention of Money-laundering (Maintenance of Records) Rules, 2005, as amended from time to time.
14. **"Senior Management"** for the purpose of this Policy shall mean the Directors of the Company, as applicable.
15. **"Suspicious Transactions"** shall have the meaning given to such term in the Master Directions and any other regulations, guidelines, and /or circulars as may be issued by RBI.
16. "**Interoperability**" means that regardless of who issues the PPI card or the e-wallet, customers can use their PPI card or e-wallet at any payment acceptance point. Therefore,it means, under interoperability, a PPI holder can swipe their card at any merchant outlet having a card swiping machine. Likewise, while UPI is interoperable, a customer would be able to transfer their NYE wallet funds to other PPI wallet if they wish, and vice versa.

1. Customer Acceptance Policy ("CAP"):

Customer Acceptance Policy lays down the criteria for acceptance of the Customers. The guidelines in respect of the Customer relationship in the Company broadly includes the following:

1.1. No account is to be opened in anonymous or fictitious / benami name(s) / entity (ies);

1.2. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished. All Accounts shall undergo CDD, KYC & AML processes and records of the same shall be maintained. Discrepancies to these processes shall be recorded and reported.

1.3. No transaction or account-based relationship is undertaken without: (a) following the Customer Identification Procedure and Risk Management.

1.4. CDD procedure shall be applied at the Unique Customer Identification Code (UCIC) level.

1.5. CDD Procedure shall be applicable for all the joint account holders, while opening a joint account.

1.6. Any mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, shall be clearly specified.

1.7. Any optional / additional information should be sought separately with consent, clearly indicating that providing of such information is optional.

1.8. Necessary checks should be carried out 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, etc, or with Persons whose name appears in the sanctions lists circulated by the RBI.

1.9. Documentation requirements and other information to be collected in respect of different categories of the Customers and keeping in mind the requirements of PMLA Act and the guidelines issued by RBI and other statutory and regulatory bodies from time to time. Every customer onboarding shall be done as per internal AML checklist and customers if listed in negative lists (including politically exposed persons, BSE/NSE defaulters, income tax defaulters, CIBIL defaulters, absconding criminals, etc), shall not be onboarded.

1.10. Every account opened is also categorized into Low, Medium and High risk as per the company's risk policy.

1.11. While implementation of Customer Acceptance Policy is necessary, such procedures should not become too restrictive and result in denial of the Company services to general public, especially those, who are financially or socially disadvantaged

1.12. Agents, through whom the business is conducted and who may be the customer as well, work on the pre-paid model with the Company have been classified as Low Risk customers.

1.13. The customer profile will be treated as a confidential and details contained therein will not be divulged to outsiders for cross selling or any other purposes.

1.14. The responsibility of ensuring compliance in relation to customer acceptance policy shall be with the Sales / Business Development Team of the Company

2. Customer Identification Procedures ("CIP"):

2.1 Customer identification means identifying the Customer and verifying their identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to verify the identity of each new Customer. Besides risk perception, the nature of information/documents required would also depend on the type of the Customer (individual, corporate, etc.). For the Customers that are natural persons, the Company shall obtain sufficient identification data to verify the identity of the Customer, their address/location, and live photograph.

2.2 The KYC checklist / documents and information to be obtained from Customers shall be in line with Annexure II of this Policy; KYC process followed by the Company has been enumerated below:

2.3 KYC Rejection

Request for KYC updation will be rejected on the following conditions:

2.3.1 Information furnished by the user does not match with the document/s furnished/ uploaded.

2.3.2 Furnished documentation is not complete, has invalid/expired documentation or copies furnished are illegible.

2.3.3 Photograph captured does not match with the correct formats as displayed in the below pictorial presentation.

2.4 KYC Updation

2.4.1 For KYC updation, a request will be sent by the user via email to the RapiPay Support Team at nyecare@RapiPay.com along with complete, clear and valid documents or upload the valid documents through mobile app or website to update against his/her record stored with RapiPay. After due scrutiny of the documents, the information will be updated.

2.4.2 KYC updation confirmation via web/App/mail will be sent to all low risk users once every five years and to all medium and high risk users once every two years.

2.4 Wallet Reactivation Reporting

Rapipay will notify RBI on the wallets which are reactivated.

2.5 In addition, if applicable, Enhanced Customer Identification Requirements keeping in view the provisions PML Act as indicated in Annexure I hereto, shall also be adhered to while undertaking Customer Identification Procedure.

2.6 The responsibility of ensuring compliance in relation to customer identification policy shall be with the Operations / Compliance Team of the Company.

2.7 Allotment of Unique Customer Identification Code (UCIC):

The Company shall allot a Unique Customer Identification Code ("UCIC") to all its new Customers while entering into a relationship. Further for the existing Customers such UCIC would be created, as required in terms of the applicable laws and / or RBI regulations. The UCIC will be used to identify Customers, avoid multiple identities and monitor financial transactions in a holistic manner.

2.8 All PPIs should have a minimum validity of 10 years PPI issuer shall caution the PPI holder at reasonable intervals, during the 45 days' period prior to expiry of the validity period of the PPI. The caution advice shall be sent by SMS / e-mail / any other means in the language preferred by the holder indicated at the time of issuance of the PPI.

2.9 The PPI Issuer shall clearly indicate the expiry period of the PPI to the customer at the time of issuance of PPIs. Such information shall be clearly enunciated in the terms and conditions of sale of PPI. Where applicable, it shall also be clearly outlined on the website / mobile application of the PPI issuer.

2.10 PIs with no financial transaction for a consecutive period of one year shall be made inactive by the PPI issuer after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence. These PPIs shall be reported to RBI separately.

2.11 The holders of PPIs shall be permitted to redeem the outstanding balance in the PPI, if for any reason the scheme is being wound-up or is directed by RBI to be discontinued.

3 Monitoring of Transactions:

3.1 Ongoing monitoring / ongoing due diligence is an essential element of effective implementation of this Policy. The Company shall make an endeavor to understand the normal and reasonable activity of the Agent and Customer so that transactions which fall outside the regular/pattern of activity can be identified. Monitoring of transactions shall be conducted by the Operations Team of the Company.

3.2 Special attention shall be paid to certain categories of transactions such as those which are complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. The transactions that involve large amounts of cash inconsistent with the normal and expected activity of the Agent and / or Customer should particularly attract the attention of the Company.

3.3 The Operation / Compliance Team of the Company shall carry out the periodic review of performance of agents, risk categorization of transactions/Customer's accounts and the need for applying enhanced due diligence measures at a periodicity of not less than annual basis.

3.4 The responsibility of ensuring compliance in relation to monitoring of transactions/ ongoing due diligence shall be with the Sales / Business Development Team of the Company.

4 **Risk Management**:

4.1 The responsibility of ensuring compliance in relation to monitoring of transactions / ongoing due diligence shall be with the Operations / Risk team of the Company.

4.2 The responsibility of ensuring compliance in relation to monitoring of transactions / ongoing due diligence shall be with the Operations / Risk team of the Company.

4.3 Rapipay will create risk profiles based on the various AML measures keeping in view the risks involved in a transaction, account or business relationship in relation to each Customer.

4.4 There shall be a cooling period of 5 minutes for funds transfer upon opening the wallet so as to mitigate the fraudulent use of the wallet. Also there should be limit imposed on the number of beneficiaries added, alerting the customers through SMS/Email each time a beneficiary is added.

4.5 For Wallet to Bank Interoperable transfers, cooling period of 30 mins to be allowed, after customer adds beneficiary.

4.6 Issuer shall provide customer induced options for fixing a cap on number of transaction values for different types of transactions/beneficiaries. Customers shall be allowed to change the caps, with additional authentication and validation.

4.7 Velocity check for transactions and other suitable measures to prevent, detect and restrict occurrence of fraudulent transactions and have an escalation mechanism in place (other than alerting the customer) for such transactions.

4.8 On onboarding, customers shall be categorized as low, medium or high risk category, based on the risk perception assessment by RFPL. Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, etc

4.9 Carry out Money Laundering(ML) and Terrorist Financing (TF) Risk Assessment exercise during Customer/ Agent onboarding as well as 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

5 **Security Management:**

5.1 Appropriate Mechanisms to restrict invalid access/login attempts, inactivity, timeout features, etc on all digital platforms

5.2 Issuer shall introduce a system where all wallet transactions involving debit to the wallet, including cash withdrawal transactions, shall be permitted only by validation through a Two Factor Authentication (2FA). -- achieved by device binding and also login to Rapipay wallet app using PIN/Password?

5.3 The Additional Factor of Authentication (AFA) requirements for PPI Cards (physical or virtual) shall be same as required for debit cards.

5.4 Keeping in view the changing payment needs and the requirement to balance the safety and security of card transactions with customer convenience, it has been decided to permit processing of e-mandate on cards for recurring transactions (merchant payments) with AFA during e-mandate registration, modification and revocation, as also for the first transaction, and simple / automatic subsequent successive transactions, subject to conditions listed in the Annex. The maximum permissible limit will be as the regulator

6 Customer Grievance/Dispute Redressal

6.1 Details of Charges and Fees structure is displayed on App and Website under the Terms and Usage policy.

6.2 In case of any complaints / feedback / query, user can reach out to customer services at RFPL from App or Website with the following details:

6.2.1 For UPI, CASA Accounts, PPI wallet/card, Loan, Bill Payment, Money Transfer, Payment related issues:

Level 1:

User can write to nyecare@rapipay.com
Phone number:0120-6366034
First response to a user's query/ concern 24hrs

Level 2:

If the resolution received does not meet user's expectations, s/he can write to nyeservicehead@rapipay.com
Follow-up queries 48hrs

Level 3:
If user is still not satisfied, s/he can write to:
Jithin Karkera

Grievance Nodal Officer
Phone No: +91 120 6366011
Email: grievanceofficer@rapipay.com
Address: RapiPay Fintech Private Limited A-8, 8thFloor, (Q-Tower),
Sector-68, Noida-201301
Customer grievances 21days

6.3 Estimated time taken to address user's queries, concerns, complaints –

7 PPI Interoperability Policies

7.1 Interoperability of PPI is enabled using UPI for Full KYC holders. It is also enabled through card using Rupay and all cards are EMV Pin and Chip Compliant.

7.2 Only Customer wallets are linked to UPI handles issued by NPCI.

7.3 Authentication shall be completed by the PPI holder as per her/his existing wallet credentials. In other words, a transaction shall be pre-approved before it reaches UPI.

7.4 For the purpose of settlement, Rapipay shall participate through a Sponsored bank and shall follow all requirements laid down by the bank to provide UPI functionality

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 Rule 3 of the PML Rules.

8.2 The records required to be maintained in relation to the transactions mentioned above shall contain the following information

8.2.1 the nature of the transactions
8.2.2 the amount of the transaction and the currency in which it was denominated;
8.2.3 the date on which the transaction was conducted;
8.2.4 the parties to the transaction

8.3 Preservation of records:

8.3.1 The electronic information provided for KYC is stored in an encrypted format on the Company's server which is archived to the local repository on a weekly basis (7 days of the documents are uploaded). All the data which has been archived is moved from the server and stored on the encrypted local repository. Any KYC request pending for more than 7 days, the data gets archived and stored in an encrypted format on the local repository, and the Company will reject the request and the user will be prompted to do the KYC again.

8.3.2 Company shall maintain a log of all the transactions undertaken for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI. Company shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND).

8.3.3 Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information (in hard and/or soft copies) in a manner that allows such data to be retrieved easily and quickly whenever required or as and when requested by competent authorities.

8.3.4 The Compliance Team of the Company shall be responsible of compliance of the above provisions in relation to Record Keeping and preservation of record.

9 Compliance of this Policy

9.1 The Company shall have an ongoing employee training program so that the members of the staff and its Agents are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new agents. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

9.2 The Senior Management of the Company under the supervision of the Board of Directors and any committee of the Company shall ensure effective implementation of this Policy by putting in place appropriate procedures to ensuring their effective implementation, covering proper management oversight, systems and controls, segregation of duties, training and other related matters.

9.3 The Company shall utilize risk-based approach to address management and mitigation of various AML risks and ensure concurrent/internal audit and independent evaluation to verify the compliance with this Policy and procedures, including legal and regulatory compliances under the PML Act, PML Rules, the guidelines issued by RBI and other statutory and regulatory bodies from time to time.

9.4 The Company shall put in place a concurrent / internal audit system to verify compliances with KYC / AML policies and procedures and shall also ensure independent evaluation of the Company's policies and procedures, including legal and regulatory requirements.

9.5 Further, the Company shall have an adequate screening mechanism in place as an integral part of its recruitment/ hiring process to ensure that persons of criminal nature or background do not get an access, to misuse the financial channel. The Head of Human Resources of the Company shall be responsible for compliance of this provision.

9.6 The Compliance Team of the Company shall submit on a quarterly basis, audit notes and compliance to the Board of Directors of the Company.

10 Designated Director

The Company shall appoint a person who is the Managing Director or a whole time Director, (but other than the Principal Officer), as the "Designated Director", to ensure compliance with the obligations under the PML Act and PML Rules. The name, designation and address of such 'designated director', may be communicated to the FIU-IND.

11 Appointment of Principal Officer

The Company shall designate a senior employee as the 'Principal Officer' ("Principal Officer") who shall be located at the Head / Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer shall maintain close liaison with enforcement agencies, NBFCs and any other institutions which are involved in the fight against money laundering and combating financing of terrorism. The employees of the Company shall endeavor to provide any information in relation to suspicious transactions, on receipt of any notices / other information in relation thereto to the Principal Officer.

12 Reporting to Financial Intelligence Unit – India

The Principal Officer shall report information relating to Suspicious Transactions, if detected, to the Director, Financial Intelligence Unit - India (FIU-IND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI

The employees of the Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions and it shall be ensured that there is no tipping off / information leak to the Customer at any level. A copy of information furnished shall be retained by the Principal Officer for the purposes of official record.

13 MISCELLANEOUS

13.1 Introduction of new technologies

The Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favor anonymity, and take measures, if needed, to prevent their use in money laundering. The Company shall ensure that any remittance of funds by any other mode, for any amount, is affected by debit to the Customer's account and not against cash payment.

13.2 KYC for the Existing Accounts

While this Policy will apply to all new Agents and Customers, the same would also be applied to the existing Agents and Customers based on materiality and risk. However, transactions with existing Agents and Customers would be continuously monitored for any unusual pattern in the operation of the accounts.

13.3 Conflict / Modification

The contents of this Policy shall always be read in conjunction with the Master Directions and / or other laws, rules, regulations and guidelines issued in this regard, from time to time and in the event of any change in the Master Directions and / or other laws, rules, regulations and guidelines, this Policy shall ipso facto stand amended to the extent required.

ANNEXURE I

CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

Accounts of Politically Exposed Persons (PEPs) resident outside India:

PEPs, or politically exposed persons are 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. The Company shall gather sufficient information on any Person of this category intending to establish a relationship and check all the information available on the Person in the public domain. The Company shall verify the identity of the Person and seek sufficient information including information about the sources of funds, accounts of the family members and/or close relatives of the PEPs, before accepting the PEP as a Customer. The decision to provide financial services to an account for the PEP shall be taken by the Board/Management Committee, in accordance with the Customer Acceptance Policy and shall be subjected to enhanced monitoring on an ongoing basis. In the event of an existing Customer or the Beneficial Owner of an existing account subsequently becoming a PEP, approval of the Board/Management Committee shall be obtained to continue the business relationship. The above norms shall also be applied to the accounts where the PEP is a Beneficial Owner.

Trust/Nominee or Fiduciary Accounts:

Branch offices shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the Persons on whose behalf they are reacting, as also obtain details of the nature of the trust or other arrangements in place. The Company shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any Person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined.

Accounts of companies and firms:

Branch offices need to be vigilant against business entities being used by individuals as a front for maintaining accounts with the Company and / or other NBFCs. Branch offices may 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. When the Company identifies a Customer (which is a company / firm) for opening an account, it should identify the Beneficial Owners of such Customer and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify the identity.

ANNEXURE II

Customer Identification Procedure Features to be verified and documents that shall be obtained

FULL KYC Checklist	
Features	**Documents (Certified copy)**
Individuals: Legal name and any other names used	1. Passport 2. PAN card 3. Voter's Identity Card 4. Aadhar Card issued by UIDAI 5. Driving license
Correct permanent address	1. Aadhar Card issued by UIDAI (any one document which provides customer information to the satisfaction of the Company will suffice) One recent passport size photograph except in case of transactions referred to in Rule 9(1)(b) of the PML Rules.

'Officially valid document' is defined to mean the passport, the driving license, the permanent account number card, the Voter's Identity Card issued by the Election Commission of India or any other document as may be required by the Company.

ANNEXURE *III*

Money Laundering and Terrorist Financing Risk Assessment

Background:

The Reserve Bank of India **(RBI)** introduced an amendment to Master Direction – Know Your Customer (KYC) Direction, 2016 requiring regulated entities to carry out money laundering **(ML)** and terrorist financing **(TF)** risk assessment exercises periodically. This requirement shall be applicable with immediate effect and the first assessment shall be carried out by June 30, 2020.

Undertaking ML and TF risk assessment is a very subjective matter with no standard process to be followed for the same. There is no uniformity on procedures of risk assessment, however, the Company has considered guidance principles enumerated by international bodies for carrying out risk assessment exercise.

Global practices for ML/TF risk assessment:

The concept of ML and TF risk assessment arises from the recommendations of Financial Action Task Force **(FATF)**. Based on FATF recommendations, many jurisdictions have prepared and published risk assessment procedures. India is yet to come up with the same. For example, the national risk assessment of money laundering and terrorist financing is the guidance published by the UK government which provides for sector specific guidance for risk assessment. The sector specific guidance is further granulated keeping in view the specific threats to certain parts of the sector.

Risk assessment process:

The Company has domestic operations and its Customers fall into similar categories and/or where the range of products and services are homogenous and hence a simple risk assessment suffices. The Company is primarily into prepaid payment instruments, facilitating money transfer, cash withdrawal, payments, transactions, through a Business to Business and Business to Customer mechanism using IT mobile based application. In addition to the customer identification procedures as per the Policy approved by the Board, the process of ML / TF risk assessment may be divided into following steps:

Step 1: Collection of information:

- The risk assessment shall begin with collecting of information on a wide range of variables including information on the general criminal environment, TF and terrorism threats, TF vulnerabilities of specific sectors and products, and the general anti-money laundering **(AML)** measures in place.

- The information may be collected externally or internally. It can be fetched through the FI being carried out for the borrower through external empaneled agency. They have repository of records and dedup on same along with google database gives a desired outcome. Any negative remark in this report shall be taken into account by credit team while underwriting the loan proposal.

Step 2: Threat identification

- Based on the information collected, jurisdiction and sector specific threats would be identified based on the risks identified on the national level; however, it shall not be limited to the same and shall be commensurate to the size and nature of business.

- Factors to be considered include the level of inherent risk including the nature and complexity of the Company's loan products and services, size, business model, corporate governance arrangements, delivery channels among others. Focus would also be given to the internal controls in place and the functioning of the internal oversight functions.

Step 3: Assessment of ML/TF vulnerabilities:

- This step involves determination of the how the identified threats will impact the entity / borrower with the probability of risks occurring. Based on the assessment, ML/TF risks should be classified as low, medium and high impact risks.

- While assessing the risks, following indicative factors should be considered:
  - The nature, scale, diversity and complexity of business and target markets;
  - The number of Customers already identified as high risk;
  - The jurisdictions the Company is exposed to, either through its own activities or the activities of Customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by RBI or FATF;
  - The distribution channels, including the extent to which the Company relies on third parties / business associates to conduct Customer Due Diligence (CDD);
  - The internal audit and regulatory findings

- This information should be supplemented with information obtained from relevant internal and external sources, such as operational/business heads and lists issued by inter-governmental international organisations, national governments and regulators.

Step 4: Analysis of ML/TF threats and vulnerabilities:

Once potential TF threats and vulnerabilities are identified, the next step is to consider how these interact to form risks including assessment of likely consequences.

Step 5: Risk Mitigation:

Post the analysis of threats and vulnerabilities, appropriate mitigant for the ML/TF risks identified shall be put in place. The initial stages of the CDD process helps to assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

Risk identification and its mitigation can be broadly classified based on the following:

- **Business-based risk assessment**: Company's products, services and delivery channels, the geographical location in which the Company operates along with other relevant factors, if any.

- **Products, Services and Delivery Channels**

Examples	Mitigant / Steps to consider
High-risk products and services, such as: • electronic funds transfers,./ • products offered through the use of intermediaries or agents	• Legitimate products and processes can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Steps to mitigate may involve assessment of the products and services by the type of market that they are directed to or nature of product (e.g. individuals, or corporate, personal loan etc.) as this may have an impact on the risk. • Additionally, it may be checked whether the products or services allow Customers to conduct business or transactions with higher-risk business segments, or could they be used by Customers on behalf of third parties.
Delivery channels, such as: • Non face-to-face transactions • Business Associate / Agent network	There may be a higher inherent risk with regards to delivery channels in non face-to-face transactions, use agents or if Customers can apply for products online. Adherence to strict AML norms and tracking end usage of funds till the desired party for which loan is meant helps mitigate the risk. Also additional comforting factor could be retail nature of product offering which to an extent mitigates possibility of ML / TF.
New Technologies	• Products/services that are based on new technologies may have an impact on overall inherent risks. • E.g.: new payment methods can be used to transmit funds more quickly or anonymously, such as electronic wallets, pre-paid cards, internet payment services, digital currency or mobile payments.

- **Geography**

Examples	Mitigant / Steps to consider
Border-crossings: • Air (i.e. airports) • Water (i.e. ports, marinas) • Land • Rail	If business is situated near a border-crossing, there may be a higher inherent risk due to the fact that it may be the first point of entry into the financial system. The Company does not have any such operational presence.
Geographical location and demographics: • Large city • Rural area	• Depending on situation, a rural area where Customers are known to the Company could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. • Governments database details of crime by regions may benefit the assessment. The Company has access to several database to verify and criminal proceedings or any other litigation pertaining to the borrower / individuals.
Connection to high-risk countries: • UN Security Council Resolutions • FATF list of High-Risk Countries and Non-Cooperative Jurisdictions	Certain countries should be identified as posing a high risk for ML/TF based on, among other things, their level of corruption, the prevalence of crime in their region, the weaknesses of their money laundering control regime, or being identified by competent authorities like the FATF or through their respective advisories. The Company business operations and nature of product offerings are not having presence outside India hence risk is mitigated.

- **Other Relevant Factors (If applicable)**

Examples	Mitigant / Steps to consider
• Ministerial Directives • Regulators	Sanctions can impact business by: • prohibiting trade and other economic activity with a foreign market, • restricting financial transactions such as foreign investments or acquisitions, or • leading to the seizure of property situated in India. These restrictions may apply to dealings with entire countries, non-state actors, such as terrorist organizations from a target country. Any ministerial directives must be taken into consideration and any additional measures to be followed as specified by regulator from time to time.
Business model: • Operational structure • Third party and/or service providers	• Consideration of business model, the size of business, the number of branches and employees, is required to determine if risks exist in relation to this element. E.g.: - A business with several branches and thousands of employees will present different risks than a business that has one location and 2 employees. - A business with a high employee turnover. • This highlights the fact that other compliance regime elements such as training are very much intertwined with risk-based approach exercise. Adequate training – mainly an On The Job training to underwriting team is effectively undertaken by the Company for awareness and better implementation of functional roles. • Use of a third party or service provider can be a good business practice, but the business is ultimately responsible for the compliance regime, client identification, record keeping and reporting obligations. Full understanding of how third party/service provider is functioning is required.

- **Relationship-based risk assessment**: products and services Customers utilize, the geographical locations in which asset is acquired or they do business as well as their activities, transaction patterns among others.

  - **Products, Services and Delivery Channels:** The examples as elicited above applied, mutatis-mutandis, to Customers as well.

  - **Geography**

Examples	Mitigant / Steps to consider
Customer's proximity to an office / branch	A Customer that conducts business or transactions away from its home office / branch without reasonable explanation should be noticed.
Customer is a non-resident	Identification of these Customers may prove more difficult since they may not be present in person and as such, should raise the inherent level of risk.
Customer acquiring asset under consideration away from business place / current residence	A Customer who is proposing to buy a house away from the regular business place or current residence without reasonable justification should be noticed.
Customer has offshore business activities or interests.	Is there a legitimate reason for this? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.

- **Pattern of activity**

Examples	Mitigant / Steps to consider
Customer is in possession/ control of / acquiring property that is owned/controlled by/on behalf of a terrorist/a terrorist group	This needs to be highlighted to the government authority.
Customer is a Politically Exposed Foreign Person (PEFP)	A PEFP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence that they may hold, a PEFP is vulnerable to ML/TF or other offences such as corruption. As a business, a politically exposed foreign person is a high-risk Customer.
The account activity does not match the Customer profile	Account activity that doesn't match the Customer profile may indicate a higher risk of ML/TF.
Customer's business generates cash for transactions not normally cash intensive	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.

- **Focus on CDD procedure:**

  - During the CDD process that the identity of a Customer is verified and risk based assessment of the Customer is done. While assessing credit risks, ML/TF risks shall also be assessed.

  - The risk classification of the Customer, as discussed above, should also be done based on the CDD carried out. The CDD procedure, apart from verifying the identity of the Customer, should also go a few steps further to understand the nature of business or activity of the Customer. Measures should be taken to prevent the misuse of legal persons for money laundering or terrorist financing including transaction due diligence to identify source and application of funds, beneficiary of the transaction, purpose etc.

  - Records on transactions and information obtained through the CDD measures shall be maintained. The CDD information and the transaction records should be made available to competent authorities upon appropriate authority. Some examples of enhanced due diligence measures are as follows:
    - carrying out additional searches (e.g., verifiable adverse media searches)
    - commissioning an intelligence report on the Customer or beneficial owner to understand better the risk that the Customer or beneficial owner may be involved in criminal activity
    - verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
    - seeking additional information from the Customer about the purpose and intended nature of the business relationship
    - seeking information about purpose of buying asset under consideration and its relevance in correlation with data provided in loan application form.

  - **Other measures**
    - Monitoring through periodical Credit Risk Monitoring Framework (CRMF) exercises (on sample basis) also involves identifying changes to the usage of asset mortgaged, Customer profile (for example, their behavior, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures.
    - Funds / instances or transactions that are suspicious should be reported promptly to the FIU and in the manner specified by the authorities as per the KYC Policy as already approved.

Step 6: Review and update risk assessment:

Once assessed, the impact of the risk shall be recorded and measures to mitigate the same shall be documented. The information that forms basis of the risk assessment process should be timely updated and shall be put up to the risk management committee of the Company, annually, for its assessment / monitoring. The outcome of this exercise shall be made available to competent authorities and self-regulating bodies, as and when required by them. The entire risk assessment procedure should be carried out in case of major change in the information.

Annexure IV:

KYC process for customers:

KYC Process

Full KYC *(Monthly Cap of Rs. 2,00,000/-)*
For Customers
Mobile Number
Full Name
Address
State
Pincode
Pan Card or Declaration for Pan card
Document Type
Document ID (unique)
Aadhaar card
Father/Spouse's name
Date of Birth
Marital Status
Annual Income
Occupation
Live verification of all documents

A. Full KYC of a customer will start with OKYC/EKYC/Digilocker pull of Aadhaar OR CKYCR download followed by a VKYC -- which will generate a V-CIP

a. For OKYC, customer has to enter aadhaar, followed by captcha, share code and OTP to pull the xml data from UIDAI. The entire process will take place at KYC third party end and RFPL will not store aadhaar details at our end.

b. For Digilocker, customer to enter aadhaar and OTP on 3rd party platform, to pull XML data.

c. EKYC option will be provided to customer once RFPL acquires KUA/AUA license. Customer will enter aadhaar and OTP for completing EKYC.

d. KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer

KYC data of customer as obtained above will be uploaded into Central KYC repository (CKYCR) as per the Operational Guidelines released by CERSAI on a daily basis.

B. Post OKYC/Digilocker/EKYC/CKYCR, VKYC will be conducted by an employee appointed by Rapipay and V-CIP will be created in online mode-

- 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-controlled mechanism given by REs to its authorized officials.

- The RE official must inform the customer about starting a VKYC/V-CIP process for completing the full-KYC

- The RE must ensure to capture photograph of the Original PAN along with original document for proof of address (only when the customer's aadhaar address doesnt match his communication address). Post this, RE must also capture Live photograph of the customer and all the docs (PAN & OVD for address) as well as the customer's photograph shall contain a water-mark in readable form having GPS coordinate of the customer, authorized official's name, unique employee code and date/timestamp.

- RE official asks for a 4-digit code displayed on the screen of the customer

- The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured that is ensured by a live V-CIP process. 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.

- Similarly, the live photograph of the original PAN or any OCD 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.

- The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

- 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.

- 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 the customer (ii) live photograph of the customer matches with the photo available in the document. (iii) Address submitted by the customer matches the document proof furnished by the customer (iv) Liveness check of the customer has to be checked

- Customer visits RE website/application and can schedule a V-CIP or start one instantly.

- Customer receives an automated confirmation on SMS or email with joining link.

- Get a video call with RE official.

- RE official carries out the above-mentioned process.

- RE employee accepts or rejects the KYC application after verification

A. As Part of Full KYC process, a CIP can be done by an officer appointed by RapiPay in offline mode-

- Customer chooses the option for an offline CIP process.

- The RE's website/Application automatically generates a reference id and shows the customers a list of nearby agents appointed by RE for successfully completing the CIP of any customer.

- The customer can visit any nearby agent appointed by RE to finish his CIP process

- The agent asks for the reference id generated on the customer's end and enters it in the agent's system

- Upon successful authentication of the reference id, the agent starts the CIP process

- The agent takes the thumbprint of the customer by a biometric device and the system uses the APIs provided by UAIDAI to matche it with the Aadhaar details provided by the user.

- Photograph of the customer is taken by the agent through Aadhaar and further, the system Application of the RE shall put a water-mark in readable form having 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

B. As part of full KYC process, a V-CIP can also be done by an automated system that mimics the responsibilities of the authorised officer of RE in conducting the online V-CIP process. However, the final approval or rejection of the KYC process will still rest with an authorised officer of the RE. This is still under development and will be deployed only after full testing cycle of positive and negative test cases.

- Customer visits RE website/application and can schedule a V-CIP or start one instantly.
- Customer receives an automated confirmation on SMS or email with joining link.
- Get a video call with RapiPay system using RapiPay Application.
- RapiPay system carried out the above-mentioned V-CIP process –
    - User gets full information about the process before starting.
    - The system captures the photograph of the Original PAN along with original document for proof of address (only when the customer's aadhaar address doesnt match his communication address). Post this, the system also captures Live photograph of the customer with a water-mark in readable form having GPS coordinate of the customer, Name and Employee code of the authorised officer of RE/node and date/timestamp.
    - The Application shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured that is ensured by a live V-CIP process. 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.
    - Similarly, the live photograph of the original PAN or any OCD (for address verification) should be placed horizontally 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.
    - The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
    - The system asks for a 4-digit code displayed on the screen of the customer, to test liveliness.
    - The system will also ask the customer to blink twice, to make sure of the liveliness.
    - The process will re-start if any of the error conditions is met.
    - Subsequent to all these activities, the Application shall give information about the completion of the process to the customer and also generate the transaction-id/reference-id number of the process.
    - The system will use advanced face matching, optical character recognition, machine learning and artificial intelligence algorithms to verify that: - (i) information available in the picture of document is matching with the information entered by the customer (ii) live photograph of the customer matches with the photo available in the document. (iii) Address submitted by the customer matches the document proof furnished by the customer (iv) Liveness check of the customer has to be checked
    - The authorised officer of RE will be the final authority in approving this process.