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

RAPIPAY FINTECH PRIVATE LIMITED

Document Version	V.2.4
Effective Date	August 09, 2021
Owned By	Chief Technology Officer
Approved By	Board of Directors

Table of Contents	
Particulars	Page #

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 framework 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.

This Policy includes 4 (Four) key elements:

I) Customer Acceptance Policy ("CAP");
II) Customer Identification Procedures ("CIP");
III) Monitoring of Transactions;
IV) Risk Management.

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:

"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.

"AML" stands for anti-money laundering.

"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.

"CDD" or Customer Due Diligence shall mean the process of the identifying and verifying the Customers and the Beneficial Owners.

"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.

"CFT" stands for combating financing of terrorism.

"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.

"KYC" stands for know your customer.

"Master Directions" shall have the meaning given to such term in the Introduction to this Policy.

"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.

"PEP" shall mean a politically exposed person.

"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

"PML Rules" shall mean Prevention of Money-laundering (Maintenance of Records) Rules, 2005, as amended from time to time.

"Senior Management" for the purpose of this Policy shall mean the Directors of the Company, as applicable.

"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.

I) Customer Acceptance Policy ("CAP"):

1. 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.

   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.

2. 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.

3. However, 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.

4. 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.

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

II) Customer Identification Procedures ("CIP"):

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. The KYC checklist / documents and information to be obtained from Customers shall be in line with Annexure II of this Policy; provided however, in cases where Customer desiring to open an account does not have the information mentioned in Annexure II, the Company may open accounts subject to the conditions specified under Regulation 24 of the Master Directions. All such documents shall be: (a) original seen

and verified (OSV) by the officer of the Company or an authorized agent of the Company. KYC process followed by the Company has been enumerated below:

2.1. KYC Process

Minimum KYC for Customers *(Monthly Cap of Rs. 10,000/-)*	Full KYC *(Monthly Cap of Rs. 1,00,000/-)*	
	For Agents	For Customers
Mobile Number	Mobile Number	Mobile Number
Full name	Full Name	Full Name
State	Email ID	Address
Document Type	Address	State
Document Number	State	Pincode
	Pin code	Pan Card or Declaration for Pan card
	Pan Card	Document Type
	Document Type	Document ID (unique)
	Document Number (unique)	

2.1.1. Minimum KYC for Customers

As per the PPI Direction, the minimum details include mobile number verified with One Time Pin (OTP) and self-declaration of name and unique identification number of any of the 'officially valid document' defined under Rule 2(d) of the PML Rules 2005, as amended from time to time. As per RBI Master Direction on KYC guidelines, Officially Valid Document (OVD) means

- Passport,
- Driving License,
- Voter's Identity Card issued by the Election Commission of India,
- Job Card issued by NREGA duly signed by an officer of the State Government,
- letter issued by the National Population Register containing details of name and address.

Wallet Limits for Minimum KYC Customers:

RapiPay wallet customers with Minimum KYC as specified above will be entitled to hold wallet balance/value of Rs. 10,000 only at any point of time and avail of a permissible total value of re- loads during any given month of Rs. 10,000 only which would be in an electronic form only.

These Customers shall be converted into Full KYC compliant within a period of 24 months from the date of issue of PPI, failing which no further credit shall be allowed in such PPIs. However, the Customer shall be allowed to use the balance available in the account.

2.1.2. Full KYC for Agents and Customers

As per the PPI Direction, the Full KYC shall be done in line with the RBI Master Direction on KYC guidelines. A brief process flow for Full KYC is given below:

(A) Identification and on boarding process for Agent

Case 1: For a Prospective Agent

- For registering a prospective agent and onboarding onto the RapiPay Network, company's employee visits the Agent and interacts, verifies and collects the requisite information and documentation from the Agent and inputs this data onto the Rapipay Portal - *agent.rapipay.com.*

- In case a request from a prospective agent is received either via email or website, along with the requisite information and documentation, a Rapipay employee visits that Agent and interacts, verifies and collects the seen and verified copies of the information and documentation and uploads it onto the Rapipay Portal - *agent.rapipay.com*.

- A maker-checker concept is implemented to verify the uploaded information and furnished documentation to authenticate, authorize and activate the agent onto RapiPay system.

Case 2: For a Prospective Agent under an Existing Agent

Prospective agent is created by an already existing agent in the Company's system in a hierarchical manner i.e. prospective agent (who is being added) gets registered under the existing agent (who is adding). In order to get and verify the information of the prospective agent being added to the system, it is necessary to perform KYC which is ensured by the following process:

Request for KYC:

- Existing Agent will put request for adding the prospective agent under him/her by filling the basic details of the agent (E.g. name, phone number which acts as the credentials for agent login).

- Subsequently, on the KYC page, the process of uploading required documents will be done.
- Documents uploaded by the Existing Agent will include documents for Address Proof (Aadhaar, Driving License, Passport, Voter ID etc.), PAN Card for ID proof, and Live photo of the New Agent holding the IDs as displayed on the Company's portal agent.rapipay.com.

- After uploading all the documents, the Existing Agent will give the consent for the KYC verification of the prospective agent being registered and declare that he/she has verified the uploaded documents with the originals; request for addition / registration of prospective agent gets registered successfully and his/her approval for KYC will be submitted successfully.

Approval of KYC:

- Approval of KYC shall be performed by Rapipay CRM User and is done through Rapipay CRM portal. This process will include verification of the furnished information and uploaded documents. Once an authorized Rapipay CRM user views, verifies and approves the KYC request, the agent can login to the portal by using his/her Registered Mobile Number and secure

password.

- **Parallel trial of advanced technology for Automated KYC Approval using AI/ML based technologies:**
  Rapipay is investing in more advanced risk technologies for KYC matching, review and approval. Such technology components will be deployed in KYC approval process initially on a trial basis to monitor effectiveness and improve accuracy. This process will include uptake of uploaded documents and auto-segmentation of documents and images for details and facial data extraction and then matching with person photographs. The system will auto-capture and fill these details and matching logic will provide score which will be filtered below a threshold for manual authorized Rapipay CRM user to validate. During trial period all cases will parallelly be validated by manual user to verify this trial. Over time, the system will learn and threshold updated for more efficient automation.

Note:

- When KYC request is being processed through mobile app then there is a provision to scan QR code from Aadhaar Card so that the user details can automatically get filled on KYC request page.

- While onboarding the Agents, they would undertake, when registering via the app, web or email, that they will: a) not charge beyond what is prescribed by the Company; and b) post a signage indicating their status as service providers for the Company and the fees for all services available at the outlet.

(B) Identification and onboarding process for Customer
Request for KYC:

- Company's Agent makes request for adding a new Customer. Any Agent of the company, whether appointed directly or otherwise as per this Policy, can make this request by filling the basic details of the Customer for registration via RapiPay portal - *agent.rapipay.com*.

- Subsequently, with the help of KYC page, the process of uploading the required documents is done. The Customer documents uploaded by the Agent includes documents for Address Proof (Aadhaar Card, PAN Card, Driving License, Passport etc.) and a Live photo of the Customer holding the ID card as displayed on the portal.

- In case of non-availability of PAN Card of the Customer, Agent can select Form 60 option. Once the documents are uploaded, an OTP is sent to the Customer's mobile. Customer provides the OTP and request for KYC is submitted successfully.

Approval of KYC:

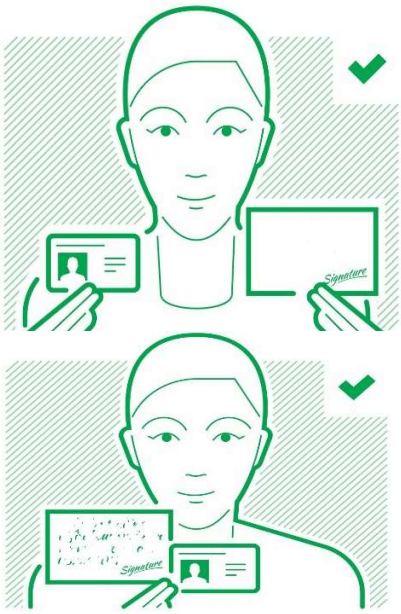
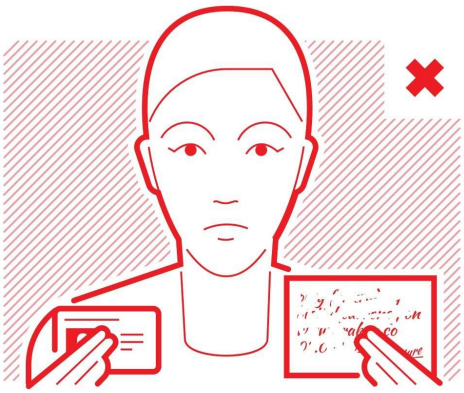
- Approval of KYC request is done by Rapipay CRM user on the Rapipay CRM portal. This process includes verification of the basic customer information and uploaded documents. After verification, the Rapipay CRM user approves the KYC of the customer.

- **Parallel trial of advanced technology for Automated KYC Approval using AI/ML based technologies:**
  Rapipay is investing in more advanced risk technologies for KYC matching, review and approval. Such technology components will be deployed in KYC approval process initially on a trial basis to monitor effectiveness and improve accuracy. This process will include uptake of uploaded documents and auto-segmentation of documents and images for details and facial data extraction and then matching with person photographs. The system will auto-capture and fill these details and matching logic will provide score which will be filtered below a threshold for manual authorized Rapipay CRM user to validate. During trial period all cases will parallelly be validated by manual user to verify this trial. Over time, the system will learn and threshold updated for more efficient automation.

Note:

- The KYC verification and updation process remains the same as above even in case its initiated via the app.

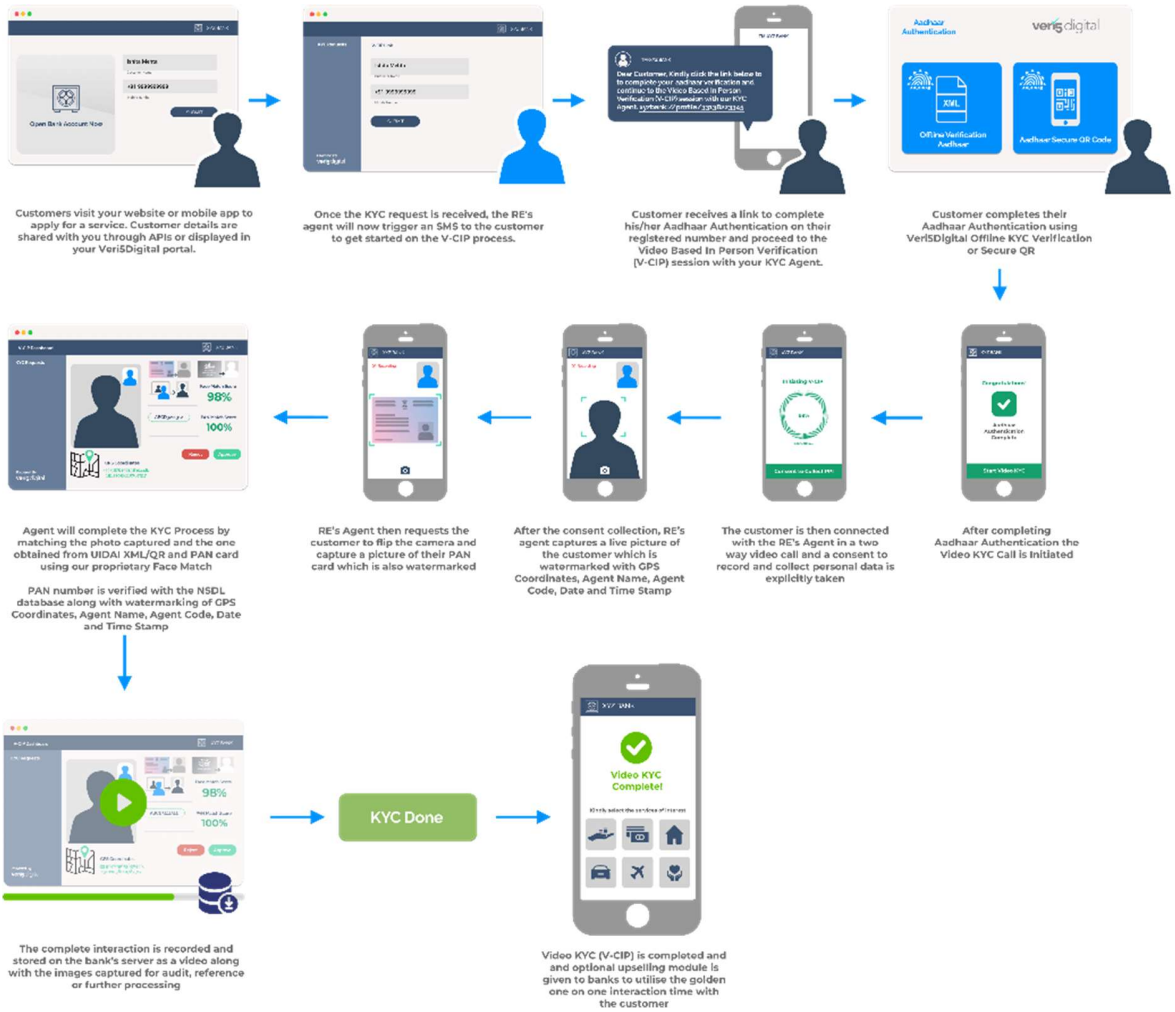
Method of taking a Live Photo

Correct	Incorrect
Live photo holding ID's (Correct) 	Live photo holding ID's (Incorrect) 
Correct Formats of the documents .jpg,.jpeg,.png	Incorrect Formats for the documents uploading .docx , .xls, .pdf,.doc
Minimum size for uploading the document is 10 KB; Maximum size for uploading the document is 8MB	Minimum size less than 10 KB Maximum size more than 8MB

2.1.3. Video KYC Process

The RBI now allows RE to digitally verify customers through Video KYC. The customer can opt for a video KYC based account opening, during which the RE official will perform identification checks along with capturing live photograph and verifying the PAN card. To avail Video KYC, the customer needs to be a resident of India, above 18 years of age and physically present in India.

(A) Customer visits RE website/application and schedule a video call.
(B) Customer receives an automated confirmation on SMS or email with joining link.
(C) Get a video call with RE official.
(D) OSV checks of official valid documents. Aadhar Card, Driving Licence, Passport, Voter ID or NREGA for POI and PAN for proof of address.
RE Official captures the Live image of customer and documents.
(E) Address verification by the customer with geo-tagging
(F) Face matching with documentation
(G) Customer image verification and validation
(H) RE employee accepts or rejects the KYC application after verification
(I) RE audit review the details and process the application
(J) Customer will be notified when KYC is successful or failed.
(K) Process flow



2.2. KYC Updation:

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

2.2.2 Agents are classified under lowrisk category and their KYC shall be updated once in every ten years.

2.2.3 **Updation from Minimum-KYC Wallet to Full KYC Wallet:** Users can also contact RapiPay Authorized Agents along with the documents. The RapiPay Agent sends the information along with the supporting documents via email to RapiPay at care@RapiPay.com for account upgradation. Upon successful verification, the account is upgraded, and the user is intimated of the same accordingly via SMS and/ or via personal enquiry at the Agent location.

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.

3. 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 recent photograph.

4. For the Customers that are legal Persons, the Company shall:
   4.1.1. verify the legal status of such Person through proper and relevant documents;
   4.1.2. verify that any person purporting to act on behalf of the legal Person is so authorized and identify and verify the identity of that Person; and
   4.1.3. understand the ownership and control structure of such legal Person and determine who are the natural persons who ultimately control such legal Person.

5. The Company has formulated and implemented Customer Identification Procedures to determine the real identity of its Customers keeping the above in view.

6. 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.

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

8. Identification of Beneficial Owner:

For opening an account of a legal Person who is not a natural Person, the ultimate Beneficial Owner shall be identified and all reasonable steps in terms of Rule 9(3) of the PML Rules, to verify his/her identity shall be undertaken.

Sr. No.	Persons	Criteria for Beneficial Ownership
1.	Company	natural person(s), who, whether acting alone or jointly, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means 'Controlling ownership interest' would mean entitlement to more than 25% (Twenty Five Percent) of the shares or capital or profits of the company; and 'Control' shall mean 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 voting agreements
2.	Trusts	the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee and the beneficiaries with 15% (Fifteen Percent) 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
3.	Partnership firm	the natural person(s), who, whether acting alone or together, or through one or more juridical person have ownership of / entitlement to more than 15% (Fifteen Percent) share in the capital or profits of the partnership
4.	Body of Individuals or unincorporated associations	the natural person(s), who, whether acting alone or together, or through one or more juridical person, have ownership of / entitlement to 15% (Fifteen Percent) of the property or capital or profits of body of individuals or unincorporated associations. Explanation: the term 'body of individuals' includes societies.

Where no natural person is identified under points 1, 3 and 4 above, the Beneficial Owner is the relevant natural person who holds the position of senior managing official.

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 ultimate natural Beneficial Owner of such companies.

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 shall be 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.

9. 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.

III) Monitoring of Transactions:

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.

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. The Sales / Business Development 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.

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.

IV) Risk Management:

1. 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. Sales personnel shall be responsible for creating risk profiles of its existing and new agents and apply various AML measures

keeping in view the risks involved in a transaction, account or business relationship in relation to each agent and / or Customer.

2. 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.

V) Record Keeping

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.

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

1. the nature of the transactions;
2. the amount of the transaction and the currency in which it was denominated;
3. the date on which the transaction was conducted;
4. the parties to the transaction.

2. Preservation of records:

2.2.1 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.

2.2.2 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).

2.2.3 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.

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

VI) Compliance of this Policy

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.

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.

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.

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.

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.

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.

VII) 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.

VIII)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.

IX) 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.

X) MISCELLANEOUS

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.

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.

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 Correct permanent address	 1. Passport 2. PAN card 3. Voter's Identity Card 4. Aadhar Card issued by UIDAI 5. Driving license 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.
Companies- Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	1. Certificate of incorporation 2. Memorandum & Articles of Association 3. Resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact business on its behalf 4. an officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf. 5. Telephone Bill.
Partnership Firms Legal name - Address - Names of all partners and their addresses Telephone numbers of the firm and partners	1. Registration certificate, if registered 2. Partnership deed 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4. Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses. 5. Telephone Bill in the name of firm/partners.

Trusts & Foundations Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	1. Certificate of registration, if registered 2. Trust deed 3. Power of Attorney granted to transact business on its behalf 4. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses. 5. Resolution of the managing body of the foundation/association. 6. Telephone Bill.
Unincorporated association or a body of individuals	1. resolution of the managing body of such association or body of individuals 2. power of attorney granted to him to transact on its behalf 3. an officially valid document in respect of the person holding an attorney to transact on its behalf 4. and such other information as may be required by Company to collectively establish the legal existence of such as association or body of individuals.

'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.