

KHATABOOK TECHNOLOGIES PRIVATE LIMITED

MERCHANT ONBOARDING POLICY

(w.e.f. November 21, 2025)

Khatabook The logo for Khatabook PAY, featuring the word "PAY" in white capital letters inside a red rectangular box.

KHATABOOK TECHNOLOGIES PRIVATE LIMITED
CIN: U72900KA2022FTC165927

KHATABOOK TECHNOLOGIES PRIVATE LIMITED

Document Title	Merchant Onboarding Policy
Originally Framed	13th October, 2025
Last Revised Date	21st November, 2025
Current Revision Date	21st November, 2025
Authority approving the Policy	Board of Directors

1. INTRODUCTION:

Khatabook Technologies Private Limited (hereinafter referred to as "the Company", "KTPL", "we", "us", or "our") is a Reserve Bank of India (RBI) regulated Payment Aggregator (PA) committed to providing secure, reliable, and efficient payment solutions to businesses across India, with a special focus on the Micro, Small and Medium Enterprise ("MSME") sector.

The Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025 ("PA Directions") mandate that every Payment Aggregator establish a comprehensive framework for the due diligence and onboarding of merchants to prevent fraud, money laundering, and other financial crimes . This Merchant Onboarding Policy ("Policy") sets out the procedures for screening, identifying, verifying, and contracting with new merchants.

This Policy is designed to be transparent and accessible to all prospective and existing merchants. It must be read in conjunction with KTPL's KYC & AML Policy, Privacy Policy, Grievance Redressal Policy, and the Merchant Service Agreement .

2. POLICY OBJECTIVES

The objectives of this Policy are:

- a) **Regulatory Compliance:** To ensure strict adherence to the RBI PA Directions, 2025, the Master Direction on KYC, 2016 (as amended), and the Prevention of Money Laundering Act (PMLA), 2002.
- b) **Risk Mitigation:** To ensure that only legitimate merchants are onboarded, thereby mitigating financial, operational, legal, and reputational risks associated with fraudulent or illegal activities.
- c) **Customer Protection:** To protect end-customers by ensuring that merchants adhere to fair business practices, including transparent refund, return, and cancellation policies .
- d) **Transparency:** To provide merchants with a clear understanding of the onboarding process, documentation requirements, and ongoing obligations.
- e) **Trust and Integrity:** To uphold the integrity of the digital payment ecosystem by preventing KTPL's platform from being used for prohibited activities, money laundering, or terrorist financing.

3. DEFINITIONS

For the purpose of this Policy, the following definitions shall apply:

Term	Definition
Merchant	A legal entity or sole proprietor that has entered into or seeks to enter into a contract with KTPL for availing Payment Aggregator services .
Customer	The end-user (payer) who purchases goods or services from a Merchant using KTPL's payment services.
Customer Due Diligence (CDD)	The process of identifying and verifying the merchant and its beneficial owners using Officially Valid Documents (OVDs).
Officially Valid Document (OVD)	Documents including Passport, Driving Licence, proof of possession of Aadhaar number, Voter's Identity Card issued by Election Commission of India, NREGA Job Card, or letter issued by the National Population Register containing details of name and address.
Beneficial Owner (BO)	The natural person who ultimately owns or controls a legal entity, directly or indirectly through ownership of more than

	10% of shares or capital, or who exercises control through other means .
Merchant Category Code (MCC)	A four-digit code assigned to a merchant based on the type of business or services provided.
CKYCR	Central KYC Records Registry – a centralized repository of KYC records maintained by RBI .
Politically Exposed Person (PEP)	Individuals entrusted with prominent public functions by a foreign country, including heads of states, senior politicians, senior government officials, and their family members or close associates .
Light KYC	A simplified due diligence process applicable to small merchants with domestic turnover ≤ ₹40 lakh or export turnover ≤ ₹5 lakh .

4. MERCHANT ACCEPTANCE CRITERIA AND PROHIBITED LIST:

KTPL shall not enter into business relationships with unethical, illegal, or high-risk entities that could pose a threat to the integrity of the payment ecosystem. The following principles guide merchant acceptance:

- a) Legitimate Business: The merchant must be engaged in a lawful business activity with all necessary registrations and licenses.
- b) Identity Verification: The merchant's identity, address, and legal existence must be verifiable through reliable, independent documents.
- c) No Anonymous Accounts: KTPL shall not onboard any merchant operating under an anonymous, fictitious, or benami name.
- d) Sanctions Screening: All merchants, their directors, partners, and beneficial owners shall be screened against sanctions lists and domestic watchlists circulated by the Ministry of Home Affairs and any other regulatory or government agencies if any match occurs the merchant shall be rejected and, where required the same shall be reported to authorities without intimating the merchant
- e) Non-Cooperation: If a merchant fails to provide required information or documents, or if the information provided is found to be unreliable or incomplete, the onboarding application shall be rejected.

5. PROHIBITED BUSINESS CATEGORIES:

KTPL maintains a Prohibited List of business categories that are strictly prohibited from being onboarded. This list is reviewed and updated periodically based on regulatory changes and risk assessments. Merchants engaged in the following categories shall be automatically rejected:

Category	Examples
Illegal Goods and Services	Narcotics, psychotropic substances, unlicensed weapons, counterfeit goods, stolen goods.
Gambling and Betting	Online casinos, sports betting, poker, lottery tickets, fantasy sports where prohibited by law.
Adult Content	Pornography, adult entertainment, escort services, adult dating platforms.
Unauthorized Financial Services	Unlicensed forex trading, ponzi schemes, pyramid schemes, unauthorized lending, binary options.
Intellectual Property Violations	Sale of counterfeit branded goods, pirated software, media, or digital content.

Weapons and Armaments	Firearms, ammunition, explosives, military-grade equipment.
Multi-Level Marketing	Pyramid schemes, chain marketing schemes, get-rich-quick schemes.
Human Organ Trade	Sale of human organs or tissues.

6. KYC AND DUE DILIGENCE PROCEDURES:

KTPL shall conduct Customer Due Diligence (CDD) for all merchants at the time of onboarding. The extent of due diligence depends on the merchant's turnover and risk profile, as per the RBI PA Directions, 2025.

6.1 FULL KYC PROCESS

For all merchants except those qualifying for Light KYC, KTPL shall perform full KYC as per RBI norms. The mandatory components are as follows:

Component	Requirement
PAN Verification	PAN Card of the entity or proprietor is mandatory and shall be verified from the Income Tax Department's portal.
CKYCR Integration	KTPL shall register KYC data of all new merchants with the Central KYC Records Registry (CKYCR). Where available, KTPL shall download KYC records using the KYC Identifier to avoid duplication.
Settlement Bank Account Verification	A current account in the legal name of the entity or proprietor shall be verified through a cancelled cheque, bank statement, or passbook. Penny-drop verification shall be conducted to confirm account ownership.
Business Address Verification	Verification of the merchant's registered and/or operational business address shall be conducted. For high-risk merchants, physical Contact Point Verification (CPV) shall be undertaken.
Sanctions and PEP Screening	All merchants and associated individuals shall be screened against sanctions lists (UNSC, OFAC) and PEP lists at the time of onboarding and periodically thereafter.

6.2 DOCUMENTATION REQUIREMENTS BY MERCHANT TYPE

Merchant Constitution	Entity Documents Required	Individual Documents Required
Sole Proprietorship	Proof of Business (any one): GST Certificate, Shop & Establishment Certificate, Udyam Registration, or any two of: latest Utility Bill, ITR, Business Licence.	PAN Card of Proprietor, OVD of Proprietor (Aadhaar / Passport / Voter ID / Driving Licence).
Partnership Firm	Partnership Deed, PAN Card of Firm, Registration Certificate (if registered), GST Certificate (if applicable), List of Partners with authorisation letter.	PAN Card and OVD of all Partners and Authorised Signatories.
Private / Public Ltd. Company	Certificate of Incorporation, Memorandum and Articles of Association, PAN Card of Company, Board Resolution	PAN Card and OVD of all Directors and Beneficial Owners (>10% shareholding).

	authorising account operation, List of Directors.	
LLP	LLP Agreement, Certificate of Incorporation, PAN Card of LLP, GST Certificate (if applicable), List of Partners with authorisation.	PAN Card and OVD of all Designated Partners and Authorised Signatories.
Trust / Society	Trust Deed or Society Registration Certificate, PAN Card of Trust or Society, Resolution or Authorisation letter, List of Trustees or Members.	PAN Card and OVD of Authorised Signatories and Trustees with controlling interest.

6.3 LIGHT KYC PROCESS

In accordance with RBI PA Directions, 2025, merchants with a domestic turnover of up to Rs. 40 lakh or export turnover of up to Rs. 5 lakh may be onboarded through a simplified Light KYC process, which involves the following steps:

Step	Requirement
Step 1	Verify Permanent Account Number (PAN) of the entity or proprietor.
Step 2	Obtain an Officially Valid Document (OVD) of the proprietor or power of attorney holder.
Step 3	Obtain and verify at least one business KYC document such as a GST certificate, incorporation certificate, or shop establishment certificate.
Step 4	Conduct Contact Point Verification (CPV) to verify the business address.

Merchants onboarded through Light KYC shall be subject to enhanced transaction monitoring and may be required to upgrade to Full KYC if their turnover exceeds the prescribed thresholds.

6.4 VIDEO KYC (V-CIP)

KTPL may onboard merchants through the Video-based Customer Identification Process (V-CIP) as a permissible alternative to physical verification, in accordance with RBI guidelines. V-CIP shall require explicit consent of the merchant, geo-tagging to confirm location within India, a real-time liveness check, capture of live photograph and OVD images during the video call, and secure recording and storage of the entire session.

7. BUSINESS AND WEBSITE VERIFICATION

For all merchants operating an online interface, KTPL shall verify the following before activation of payment services:

Check	Requirement
Website or App URL	The URL must be functional and correctly entered. If the URL is invalid or non-functional, onboarding shall be denied.
SSL Certification	The website must be secured with a valid SSL certificate (HTTPS) to ensure data security.
About Us	A clear description of the company and the nature of its business must be prominently displayed.
Terms and Conditions	Clear and accessible terms governing the sale of goods or services, including rights and responsibilities of both merchant and customer.

Refund, Return, and Cancellation Policy	Clearly defined policies including timelines, mode of refund to original payment method, and acceptable channels for cancellation requests.
Privacy Policy	Details on how customer data is collected, used, and protected, in compliance with Indian data protection laws.
Contact Information	Legal business name, registered address, contact number, and email ID must be displayed.
Grievance Redressal Mechanism	A dedicated section detailing the process for handling customer complaints and grievances.

8. MERCHANT RISK CATEGORIZATION

All merchants shall be categorised into risk levels based on a comprehensive risk assessment. This categorisation determines the level of ongoing monitoring and due diligence required. Factors considered include the nature of business and Merchant Category Code (MCC), anticipated transaction volume and value, geographic location, legal constitution and ownership structure, prior history or adverse media reports, chargeback history, and cross-border transaction exposure.

Risk Level	Characteristics	Enhanced Measures
Low Risk	Government entities, publicly listed companies, established businesses with a long track record, low transaction values, and simple business models.	Standard monitoring, periodic KYC refresh every 3 years.
Medium Risk	Standard businesses, e-commerce platforms, and new businesses with moderate transaction volumes.	Standard monitoring, periodic KYC refresh every 2 years.
High Risk	Businesses in sectors with higher chargeback risk (e.g., travel, high-value electronics), cross-border merchants, businesses in jurisdictions with weak AML controls, and PEP-associated entities.	Enhanced Due Diligence (EDD), physical CPV, more frequent transaction monitoring, potential rolling reserve, periodic KYC refresh every 1 year.

9. TECHNICAL AND CONTRACTUAL COMPLIANCE

9.1 DATA SECURITY COMPLIANCE

Requirement	Details
PCI-DSS Compliance	Merchants processing card transactions must comply with the Payment Card Industry Data Security Standard (PCI-DSS). The compliance level required depends on annual transaction volume.
Prohibition on Card Storage	Merchants are strictly prohibited from storing customer card credentials on their servers or databases. Only KTPL or its payment processor may tokenise and store such data in compliance with RBI guidelines.
Data Localisation	All payment data must be stored only in India, as per RBI requirements.

9.2 MERCHANT AGREEMENT

A legally enforceable, comprehensive agreement must be executed between KTPL and the merchant before activation of services. The agreement shall clearly specify:

- a) Roles and responsibilities of both parties regarding payments, settlement, and chargeback processes.
- b) Clear allocation of responsibility for handling customer complaints and disputes.
- c) Obligation of the merchant to adhere to the publicised refund and cancellation policies.
- d) Fee structure, including all applicable charges.
- e) Representations and warranties regarding the legality of the merchant's business.
- f) Clauses granting KTPL the right to audit the merchant and terminate the contract upon non-compliance or breach of any regulatory requirement.
- g) Data protection and confidentiality obligations.

10. POST-ONBOARDING MONITORING

Once a merchant is onboarded, they are subject to continuous scrutiny as defined in KTPL's KYC and AML Policy. KTPL's automated fraud detection system shall continuously monitor merchant transactions for:

- a) Unusual or sudden spikes in transaction volume or value inconsistent with the merchant's profile.
- b) Transactions from high-risk jurisdictions.
- c) High chargeback ratios or unusual refund patterns.
- d) Suspicious patterns indicative of money laundering or fraud.
- e) Geo-location anomalies or velocity checks.

KTPL shall ensure that all funds are routed through the designated escrow account and that all debits and credits strictly adhere to the permissible transactions defined in the RBI PA Directions. Escrow funds shall not be combined with KTPL's corporate funds, and all debits and credits happen to the respective merchant account itself.

11. DEACTIVATION AND EXIT PROCESS

KTPL reserves the right to suspend or terminate the provision of services to a merchant under the following circumstances:

- a) Violation of Agreement: Breach of any term of the Merchant Service Agreement.
- b) Non-Compliance with KYC: Failure to complete periodic KYC updation or provide requested documents.
- c) Suspicious Activity: Detection of fraudulent, illegal, or suspicious transactions.
- d) Prohibited Business: Discovery that the merchant is engaged in a prohibited business category not disclosed at onboarding.
- e) Adverse Media: Negative media reports indicating involvement in illegal activities.
- f) Regulatory Direction: Receipt of any direction from the RBI or other regulatory authority to terminate the relationship.

The merchant shall be provided with written notice of suspension or termination and the reasons therefor, unless providing such notice would tip-off the merchant in case of suspected fraud or money laundering. Pending settlements shall be processed as per the terms of the agreement, subject to any hold required for chargeback or dispute resolution. KTPL shall retain the merchant's KYC information, transactional information, and other records as required under applicable laws, even after termination of the contract.

12. MAINTENANCE OF RECORDS

KTPL shall maintain all records relating to merchant onboarding, due diligence, and transactions as per regulatory requirements. Records shall be maintained in a manner that allows for easy retrieval and submission to the RBI or other competent authorities upon request.

Record Type	Retention Period
KYC Records (identification documents, account files, business correspondence)	At least 5 years after the business relationship ends.
Transaction Records	At least 5 years from the date of transaction.
Complaint Records	At least 10 years from closure.
STR / CTR Reports	As per FIU-IND guidelines.

13. AMENDMENT

The Company reserves the right to amend or modify this Policy, in whole or in part, at any time, subject to approval of the Board of Directors. Additionally, this Policy shall stand automatically amended to the extent necessary to give effect to any statutory modification, amendment, or revision to the applicable laws, regulations, without any further act or resolution on the part of the Company.

This Policy shall be reviewed by the Board at least once annually or upon any material regulatory or operational changes. In the event of any difficulty or doubt arising in the interpretation of this Policy, the decision of the Board of Directors shall be final, subject to applicable laws and regulations.

For Khatabook Technologies Private Limited

Date: 21st November, 2025
Place: Bengaluru

Ravish Naresh