# KHATABOOK TECHNOLOGIES PRIVATE LIMITED

## MERCHANT ONBOARDING POLICY

## (w.e.f. October 22, 2026)

# KHATABOOK TECHNOLOGIES PRIVATE LIMITED

| | |
|---|---|
| **Document Title** | **Merchant Onboarding Policy** |
| **Originally Framed** | **13th October, 2025** |
| **Last Revised Date** | **21st November, 2025** |
| **Current Revision Date** | **22nd October, 2026** |
| **Authority approving the Policy** | **Board of Directors** |

**KHATABOOK TECHNOLOGIES PRIVATE LIMITED**
**CIN: U72900KA2022FTC165927**

# 1. INTRODUCTION:

Khatabook Technologies Private Limited (hereinafter referred to as "the Company", "KTPL", "we", "us", or "our") is authorised by the Reserve Bank of India (RBI) as a Payment Aggregator – Online (PA-O) and a Payment Aggregator – Physical (PA-P), 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 carry out due diligence of the merchants it onboards, 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, whether they accept payments online (PA-O), at a physical place of business through Acceptance Devices (PA-P), or both.

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 PA Directions, 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). |

| Term | Definition |
|---|---|
| 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 centralised repository of KYC records, the functions of which are performed by the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI). |
| 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. |
| Contact Point Verification (CPV) | Physical verification of the address or place of business of the merchant. |
| Light KYC | A simplified due diligence process permitted under the PA Directions, as an alternative where the merchant's KYC record is not available in CKYCR, for merchants with annual turnover ≤ ₹40 lakh or annual export turnover ≤ ₹5 lakh. |
| PA-O (Payment Aggregator – Online) | A Payment Aggregator that facilitates transactions where the acceptance device and the payment instrument are not present in close proximity while making the transaction, such as payments on a Merchant's website, application or payment link. |
| PA-P (Payment Aggregator – Physical) | A Payment Aggregator that facilitates transactions where both the acceptance device and the payment instrument are physically present in close proximity while making the transaction. |
| Acceptance Device | A point-of-sale (POS) terminal, soundbox, QR code displayed at the Merchant's premises or any other device deployed by or through KTPL at a Merchant's physical place of business to accept payments. |
| Merchant ID (MID) / Terminal ID (TID) | Unique identifiers allotted by KTPL to a Merchant and to each Acceptance Device deployed with the Merchant, respectively. |

# 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 the 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.

f) Contractual Relationship: KTPL shall aggregate funds only for merchants with whom it has a contractual relationship, and shall not itself carry out marketplace business.

# 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, and on whether the merchant is onboarded for PA-O services, PA-P services or both, as per the PA Directions.

## 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 | With the merchant's consent, KTPL shall retrieve the merchant's KYC record from CKYCR using the KYC Identifier, to avoid duplication. Where the record is not updated, the process defined in the MD on KYC shall be followed. KTPL shall register the KYC data of all new merchants with CKYCR. |
| 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. For all PA-P merchants, physical CPV of each place of business at which an Acceptance Device is to be deployed shall be undertaken before deployment. |
| 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). |

| Merchant Constitution | Entity Documents Required | Individual Documents Required |
|---|---|---|
| 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 authorising account operation, List of Directors. | PAN Card and OVD of all Directors and Beneficial Owners (>10% shareholding). |
| 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 the PA Directions, where a merchant's KYC record is not available in CKYCR, merchants with an annual turnover of up to Rs. 40 lakh or annual 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 | Obtain a copy of the Permanent Account Number (PAN) / Form 60 of the merchant and verify the PAN from the issuing authority. |
| Step 2 | Obtain a certified copy of one Officially Valid Document (OVD) of the proprietor or of the person holding power of attorney to operate the account, as applicable. |
| Step 3 | Verify at least one of the documents, or the equivalent e-documents, prescribed for CDD of sole-proprietary firms or legal entities, 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.

### 6.5 ASSISTED MODE

In terms of the PA Directions, Digital KYC and assisted V-CIP may be carried out through Authorised Agents appointed by KTPL after due diligence, in accordance with Section 5.8 of the KYC & AML Policy. KTPL shall maintain the details of the agent who assisted each merchant, and responsibility for due diligence shall remain with KTPL.

### 6.6 MERCHANT IDENTIFIERS

KTPL shall allot an appropriate Merchant Category Code (MCC) and Merchant ID to every merchant, and a Terminal ID to each Acceptance Device deployed with a PA-P merchant, and shall ensure that the name of the merchant is captured appropriately for all transactions processed for it.

## 7. BUSINESS AND WEBSITE VERIFICATION (PA-O)

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. |

# 7A. PHYSICAL PREMISES VERIFICATION (PA-P)

For all merchants availing PA-P services, KTPL shall verify the following before deploying an Acceptance Device:

| Check | Requirement |
|---|---|
| Place of Business | The premises exist at the declared address, are operational, and are occupied by the merchant. |
| Business Activity | The goods or services observed are consistent with the declared nature of business and the MCC allotted. |
| Signage | The merchant's trade name is displayed at the premises. |
| Geo-tagging | Geo-coordinates and photographs of the premises are captured and recorded against the TID. |
| Refund and Cancellation Policy | The merchant's refund, return and cancellation policy is made available to customers at the point of sale or on the receipt. |
| Grievance Contact | Merchant and KTPL contact details are printed on charge slips or receipts. |

# 7B. ACCEPTANCE DEVICE MANAGEMENT (PA-P)

a) Acceptance Devices shall be issued only to merchants who have completed due diligence, and each device shall be mapped to a unique TID, the merchant's MID, the MCC and the verified installation address.

b) POS terminals shall be certified under the applicable PCI standards (including PCI PTS), and payment applications on them shall comply with PCI-SSF. Cryptographic keys shall be injected and managed securely.

c) KTPL shall maintain an inventory of all Acceptance Devices covering issuance, deployment, location, status and retrieval.

d) Devices shall be inspected for tampering at deployment, during periodic visits and on any alert, and device location shall be monitored where the device supports it.

e) Merchants shall not relocate, lend or transfer devices without KTPL's prior written approval, and shall report loss, theft, damage or tampering immediately.

f) Devices shall be deactivated and retrieved on suspension or termination, or when relocation, misuse or tampering is detected.

# 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 and, for PA-P merchants, the location and number of outlets, the type of Acceptance Device deployed, and the merchant's history of device misuse or relocation.

| 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 and PCI-SSF Compliance | Merchants processing card transactions must comply with the Payment Card Industry Data Security Standard (PCI-DSS) and, where applicable, the PCI Software Security Framework (PCI-SSF). The compliance level required depends on annual transaction volume. |
| Security Assessment at Onboarding | KTPL shall undertake a security assessment of the merchant during onboarding, including a review of its PCI-DSS compliance status, to ensure that baseline security controls are adhered to. |
| Prohibition on Card Storage | Merchants are strictly prohibited from storing customer card credentials on their servers or databases. In accordance with RBI directions on card-on-file tokenisation, actual card data may be stored only by card issuers and card networks; KTPL and merchants may retain only the last four digits of the card number and the card issuer's name, as permitted, for transaction tracking and reconciliation. |

| Requirement | Details |
|---|---|
| Acceptance Device Security (PA-P) | Devices and payment applications shall comply with the applicable PCI standards and PCI-SSF. Card data shall be encrypted at the point of capture, and merchants shall not record PINs, CVVs or card data. |
| 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, reconciliation, treatment of failed transactions 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 the merchant discount rate and all other applicable charges, including any set-up, rental or maintenance charges for Acceptance Devices.

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.

h) For PA-P merchants, the terms of deployment, custody, maintenance, relocation and return of Acceptance Devices.

i) Settlement timelines, stated in a fair, equitable and transparent manner.

## 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 to ensure that they are in line with the merchant's business profile, including 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.

f) For PA-P merchants: transactions from an Acceptance Device at a location other than its verified address, manually key-entered or fallback card transactions, refunds without a corresponding sale, and split or repeated card-present transactions.

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 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. In accordance with the PA Directions, the same escrow account shall be used for both PA-O and PA-P business, and it shall not be used for cash-on-delivery transactions.

## 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.

g) Device Misuse (PA-P): Relocation, tampering or misuse of an Acceptance Device, or transactions processed at a location other than the verified place of business.

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. On suspension or termination of a PA-P merchant, KTPL shall deactivate the relevant MID and TIDs and retrieve all Acceptance Devices. 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, CPV and device deployment records) | 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: 22nd October, 2026**

**Place: Bengaluru** **Ravish Naresh**