KHATABOOK TECHNOLOGIES PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING (AML) POLICY

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

KHATABOOK TECHNOLOGIES PRIVATE LIMITED

Document Title	**KYC & AML 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**

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. This Policy applies to merchants onboarded for PA-O services, PA-P services, or both.

As a Regulated Entity (RE), KTPL is obligated to establish and maintain a robust framework to prevent its platform from being used for Money Laundering (ML) or Terrorist Financing (TF) activities. The Prevention of Money Laundering Act, 2002 (PMLA) and the rules framed thereunder mandate that all financial intermediaries implement comprehensive KYC and AML procedures.

This Know Your Customer (KYC) & Anti-Money Laundering (AML) Policy outlines the principles and procedures for customer acceptance, identification, risk categorization, ongoing monitoring, and regulatory reporting. The policy is designed to be transparent, accessible, and fully compliant with all applicable laws and RBI guidelines.

2. POLICY OBJECTIVES:

The objectives of this Policy are:

a) Regulatory Compliance: To ensure strict adherence to the Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025 ("PA Directions"), the RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended ("MD on KYC"), and the Prevention of Money Laundering Act (PMLA), 2002.

b) Risk Mitigation: To prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing.

c) Customer Understanding: To enable the Company to know and understand its merchants and their financial dealings better, which in turn helps manage risks prudently.

d) Systematic Framework: To put in place an effective system and procedure for:

- Customer identification and verification based on risk factors
- Assessing and monitoring risk factors associated with each customer
- Detecting and reporting suspicious transactions

e) Integrity of Payment Ecosystem: To uphold the integrity of the digital payment ecosystem by preventing fraud, money laundering, and other financial crimes.

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.

Term	Definition
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. For a company, this means ownership of or entitlement to more than 10% of shares or capital, or control over management/policy decisions.
Central KYC Records Registry (CKYCR)	An entity defined under PML Rules to receive, store, safeguard, and retrieve KYC records in digital form of a customer.
KYC Identifier	The unique identifier generated by CKYCR for each customer based on their KYC records.
Video-Based Customer Identification Process (V-CIP)	A secure, consent-based, real-time audio-visual interaction conducted by an authorized official for customer identification and due diligence, considered equivalent to face-to-face onboarding.
Digital KYC	The process of capturing live photograph and OVDs through a secure application, with geo-tagging and validation, as specified in Annex I of the MD on KYC.
Politically Exposed Person (PEP)	Individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, and important political party officials.
Principal Officer (PO)	A senior management official nominated by the Company, responsible for ensuring KYC/AML compliance, monitoring transactions, and reporting to FIU-IND.
Designated Director (DD)	A director appointed by the Board under PMLA, responsible for overall compliance with AML obligations.
Suspicious Transaction	A transaction, including an attempted transaction, which gives rise to reasonable grounds of suspicion that it may involve proceeds of crime, appears to have no economic rationale, or may involve financing of terrorism.

Term	Definition
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.
Authorised Agent	A person appointed by KTPL, after due diligence, to assist merchants with Digital KYC and assisted V-CIP in terms of the PA Directions.

4. KEY PRINCIPLES FOR KYC:

- **No Anonymous Accounts:** No merchant account shall be opened in a name that is anonymous, fictitious, or benami.
- **Risk-Based Acceptance:** Merchants shall be accepted and activated only upon satisfactory completion of the Customer Due Diligence (CDD) process applicable to their risk category, including verification of identity and Beneficial Owners (BOs).
- **Prohibited Categories:** KTPL shall maintain a list of prohibited and restricted business categories in accordance with the Merchant Onboarding Policy. No merchant dealing in illegal, prohibited, or restricted items or services shall be onboarded.
- **Non-Cooperative Merchants:** Where KTPL is unable to complete the CDD process due to non-cooperation by the merchant, or where the information or documents furnished are unreliable or incomplete, the onboarding application shall be rejected.
- **Tipping Off:** Where the Company forms a reasonable suspicion of money laundering or terrorist financing and believes that proceeding with the Customer Due Diligence (CDD) process may tip-off the merchant, it shall immediately discontinue the CDD process and file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit India and such other regulatory or government authorities as may be required, irrespective of whether the

transaction involves cash or non-cash instruments, without alerting the merchant under any circumstances.

- **Sanctions Screening:** All merchants, their directors, partners, and beneficial owners shall be screened against the sanctions lists circulated under Section 51A of the Unlawful Activities (Prevention) Act, 1967 and the domestic watchlists circulated by the Ministry of Home Affairs (MHA) or any other government body at the time of onboarding and periodically thereafter.
- **Background and Antecedent Check:** KTPL shall conduct a background and antecedent check on every merchant prior to onboarding to assess reputational, legal, and financial risks associated with the merchant.
- **Marketplace Diligence and Fund Settlement Controls:** KTPL shall ensure that any marketplace onboarded by it does not accept payments for sellers not onboarded on the marketplace's platform and KTPL shall also put in place necessary validation mechanisms to ensure that funds due to a merchant are credited only to the merchant's verified bank account.
- **Customer Acceptance Policies (CAP):** KTPL follows a detailed KYC process, with rules and procedures setting out the approval process, the documentation required from the merchant and the factors to be considered in assessing eligibility. High-risk merchants shall be identified and approved with caution.
- **Reporting to FIU-IND:** KTPL shall maintain its registration with the Financial Intelligence Unit – India (FIU-IND) and meet the reporting requirements prescribed under the PMLA and the MD on KYC.

5. CUSTOMER DUE DILIGENCE (CDD) PROCESS:

KTPL shall undertake a comprehensive Customer Due Diligence (CDD) process, including physical or digital verification methods, at the time of commencement of the business relationship.

Component	Requirement
PAN Verification	PAN Card of the entity/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/proprietor shall be verified through a cancelled cheque, bank statement, or passbook showing the legal name, account number, and IFSC code. 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 through Contact Point Verification (CPV). For PA-P merchants, CPV shall be conducted in accordance with Section 5.7.

Component	Requirement
Beneficial Owner Identification	For legal entities, reasonable measures shall be taken to identify and verify beneficial owners (>10% shareholding/control).

5.1 FULL KYC VS. LIGHT KYC

- Full KYC shall apply to all merchants except those qualifying for Light KYC.
- Where a merchant's KYC record is not available in CKYCR, Light KYC (as per the PA Directions) may be applied as an alternative to merchants with:
  - Annual turnover ≤ ₹40 lakh, OR
  - Annual export turnover ≤ ₹5 lakh

The Light KYC process involves:

- Obtaining a copy of the PAN / Form 60 of the merchant and verifying the PAN from the issuing authority
- Conducting Contact Point Verification (CPV) of the merchant
- Obtaining a certified copy of one OVD of the proprietor or of the person holding power of attorney to operate the account, as applicable
- Verifying at least one of the documents, or the equivalent e-documents, prescribed for CDD of sole-proprietary firms or legal entities

5.2 DOCUMENTATION REQUIREMENTS FOR KYC 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 License	PAN Card of Proprietor, OVD of Proprietor (Aadhaar/Passport/Voter ID/Driving License)
Partnership Firm	Partnership Deed, PAN Card of Firm, Registration Certificate, GST Certificate (if applicable), List of Partners with authorization letter	PAN Card and OVD of all Partners and Authorized Signatories
Private/Public Ltd Company	Certificate of Incorporation, Memorandum & Articles of Association, PAN Card of Company, Board Resolution, 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, List of Partners with authorization	PAN Card and OVD of all Designated Partners and Authorized Signatories

Merchant Constitution	Entity Documents Required	Individual Documents Required
Trust/Society	Trust Deed / Society Registration Certificate, PAN Card of Trust/Society, Resolution/Authorization letter, List of Trustees/Members	PAN Card and OVD of Authorized Signatories and Trustees with controlling interest

5.3 VIDEO-BASED CUSTOMER IDENTIFICATION PROCESS (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 the MD on KYC. V-CIP shall be deemed equivalent to face-to-face onboarding for regulatory purposes. The following minimum standards shall be adhered to by KTPL, whether the V-CIP is conducted through in-house systems or through third-party tools engaged for this purpose:

Requirement	Standard
Infrastructure Housing	Technology systems must be located on the Company's own premises with secured network domains.
Data Protection	End-to-end encryption between customer devices and hosting applications with auditable consent recording.
Geographic Controls	Systems must block IP addresses from outside India and detect spoofed connections.
Location Verification	Video recordings must capture live GPS coordinates and timestamps of customer locations.
AI Integration	Face liveness detection, spoof detection, and matching technology with high accuracy levels.
Security Testing	Mandatory vulnerability assessments, penetration testing, and security audits by CERT-In-empanelled auditors.

5.4 PERMITTED USE CASES V-CIP:

- New individual merchant onboarding
- Proprietorship firm verification (proprietor identification)
- Authorized signatory verification for legal entity merchants
- Beneficial owner identification for legal entity merchants
- Periodic KYC updates for eligible merchants

5.5 MODES OF ONBOARDING:

Mode	Description	Requirements
Physical KYC	Physical verification of KYC documents by authorized officials	Original document verification, certified copies
Digital KYC	Capturing live photo and OVDs with geo-tagging, as per Annex I of the MD on KYC	Live photograph, document capture, geo-tagging

Mode	Description	Requirements
Video KYC (V-CIP)	Secure audio-visual interaction for customer identification	As per Section 5.3 above
Aadhaar OTP-based e-KYC	Authentication using OTP sent to Aadhaar-linked mobile number	Customer consent, subject to conditions

5.6 FACTORS CONSIDERED FOR RISK CATEGORIZATION:

KTPL follows a robust, risk-based approach to merchant onboarding and ongoing monitoring. All merchants shall be categorised into appropriate risk levels based on a comprehensive risk assessment, and the findings thereof shall be reported periodically to the Risk Management Committee (RMC) for review and oversight. Some of the factors considered by the Company are as follows:

- Nature of business and Merchant Category Code (MCC)
- Anticipated transaction volume and value
- Geographic location of business and customers
- Legal constitution and ownership structure
- Prior history or adverse media reports
- Chargeback history (if applicable)
- Cross-border transaction exposure
- Transactions from high-risk jurisdictions
- High chargeback ratios or unusual refund patterns
- Unusual or sudden spikes in transaction volume or value inconsistent with the merchant's profile
- For PA-P merchants: transactions from an Acceptance Device at a location other than its verified installation address
- For PA-P merchants: a high proportion of manually key-entered, fallback or repeatedly declined card-present transactions
- For PA-P merchants: refunds or reversals at a physical point of sale without a corresponding sale
- For PA-P merchants: split or repeated card-present transactions on the same card within a short interval
- For PA-P merchants: card-present transaction values or timings inconsistent with the merchant's MCC and business hours
- Any other such factor recommended by the Risk Management Committee

5.7 ADDITIONAL DUE DILIGENCE FOR PA-P MERCHANTS:

In addition to the CDD applicable to all merchants, the following shall apply to merchants onboarded for PA-P services:

- Physical CPV of every place of business at which an Acceptance Device is to be deployed shall be completed before deployment, irrespective of the merchant's risk category, including geo-tagged photographs of the premises, signage and business activity.
- The business activity observed at the premises shall be consistent with the declared nature of business and the MCC allotted.

- Each Acceptance Device shall be mapped to the merchant's MID, a unique TID, the MCC and the verified installation address. A device shall not be relocated without KTPL's prior approval and fresh CPV of the new location.
- Where a merchant operates multiple outlets, CPV shall be conducted for each outlet at which a device is deployed.
- Where a merchant avails both PA-O and PA-P services, the due diligence requirements for both shall apply.

5.8 DUE DILIGENCE THROUGH ASSISTED MODE:

In terms of the PA Directions, KTPL may use Authorised Agents only to carry out the Digital KYC process and assisted V-CIP for merchants. KTPL shall:

- carry out due diligence of every Authorised Agent before appointment;
- maintain the details of the Authorised Agent who assisted each merchant;
- not permit Authorised Agents to approve onboarding or risk categorisation; and
- retain ultimate responsibility for the due diligence of all merchants.

6. CENTRAL KYC RECORDS REGISTRY (CKYCR):

6.1 REGISTRATION WITH CKYCR:

KTPL shall register the KYC data of all new merchants and their associated individuals with the Central KYC Records Registry (CKYCR) in the prescribed format and templates.

6.2 USE OF KYC IDENTIFIER

For establishing a business relationship, KTPL shall, with the merchant’s consent, seek the KYC Identifier from the merchant to retrieve its KYC records from CKYCR.

6.3 RELIANCE ON CKYCR RECORDS

a) When downloading and relying on KYC records from CKYCR, KTPL shall not be required to re-verify the authenticity of the customer's identity and/or address, provided the records are current and compliant.

b) However, KTPL remains responsible for all other aspects of CDD, including risk categorization, ongoing due diligence, and transaction monitoring.

c) KTPL shall not rely on CKYCR records if:

- There is a change in the merchant's information
- The records retrieved are incomplete or not as per current KYC norms
- The validity period of documents has expired
- The Company deems it necessary to perform EDD

7. PERIODIC UPDATION OF KYC:

The Company shall undertake periodic updation of KYC records for all onboarded merchants based on their assigned risk category, as determined by the Company in consultation with the Risk Management Committee (RMC) and according to relevant laws and Regulations.

Risk Category	Periodicity of KYC Updation
High Risk	At least once every one (1) year
Medium Risk	At least once every two (2) years
Low Risk	At least once every three (3) years

7.1 COMMUNICATION OF RE-KYC:

The Company shall issue at least three advance notifications before the due date for re-KYC. After the due date, failure to complete KYC updation may result in restrictions on account operations, including but not limited to, suspension of settlement services.

8. MAINTENANCE OF RECORDS:

KTPL shall maintain all records pertaining to KYC, Customer Due Diligence (CDD), and associated documentation in accordance with the retention requirements prescribed under the Prevention of Money Laundering Act, 2002 (PMLA), the PA Directions, the Digital Personal Data Protection Act, 2023 (DPDP Act), and other applicable laws and regulations. All such records, including but not limited to identity documents, verification records, CPV and device deployment records, records of assisted onboarding, transaction data, risk categorisation details, and correspondence, shall be retained for such period as may be prescribed under applicable laws. Such records shall be treated as strictly confidential and shall not be disclosed to any third party except where required by law, regulation, or order of a competent authority.

9. 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**