Merchant On-boarding Policy

Computer Age Management Services Limited

For its Payments Business (CAMSPay)

Version – 1.8

CAMSPay Merchant Onboarding Policy

1. Introduction

CAMSPay, a Strategic Business Unit of Computer Age Management Services Ltd, specializes in payment aggregation. We recognize Merchant Onboarding as a critical activity within our business operations. This policy document defines the process for effectively onboarding merchants, incorporating necessary controls for our "Online Payment Aggregator business." In this capacity, we process transactions via acquiring/sponsor banks and manage settlements to merchants' authorized bank accounts.

2. Merchant Onboarding Policy Statement

CAMSPay operates as a Payment Aggregator (PA) and strictly adheres to the Reserve Bank of India (RBI) Guidelines on Regulation of Payment Aggregators and Payment Gateways (RBI/2020-21/117 CO.DPSS.POLC.No.S33/02-14-008/2020-2021).

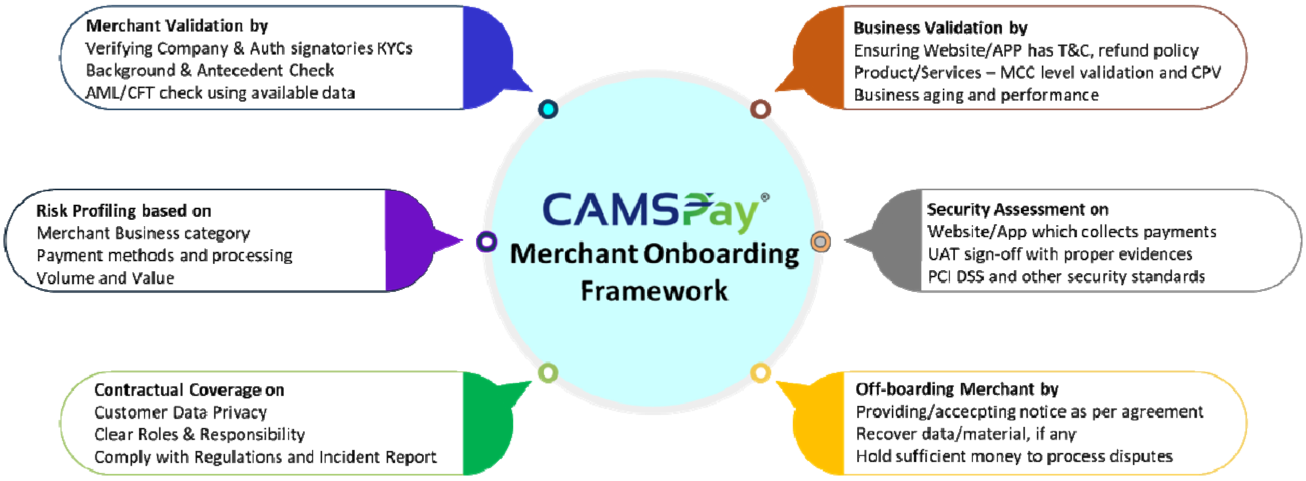
During merchant onboarding, CAMSPay collects and validates Know Your Customer (KYC) information based on the merchant's nature of business, products/services sold on their website/app, and verification that the website and mobile application include required Terms and Conditions, refund policies, contact details, and other necessary policies.

The onboarding process encompasses:

- Due diligence checks
- Assigning appropriate Merchant Category Codes (MCCs) as per banks and networks
- Risk profiling based on business and product categories
- Business background and antecedent checks
- Transaction monitoring
- Ongoing due diligence and periodic updates to ensure merchants do not engage in malafide intentions (e.g., duping customers or selling fake/counterfeit/prohibited products) using the CAMSPay platform.

CAMSPay's merchant onboarding process evaluates merchants according to prevailing KYC rules and guidelines issued by banks and regulators, applicable to the specific merchant business category. This includes screening the risk of merchants based on their business category, determining eligibility for onboarding, and smoothly onboarding qualified merchants.

Merchant Lifecycle Framework


CAMSPay
Merchant Onboarding Framework
Merchant Validation by
Verifying Company & Auth signatories KYCs
Background & Antecedent Check
AML/CFT check using available data
Business Validation by
Ensuring Website/APP has T&C, refund policy
Product/Services – MCC level validation and CPV
Business aging and performance
Risk Profiling based on
Merchant Business category
Payment methods and processing
Volume and Value
Security Assessment on
Website/App which collects payments
UAT sign-off with proper evidences
PCI DSS and other security standards
Contractual Coverage on
Customer Data Privacy
Clear Roles & Responsibility
Comply with Regulations and Incident Report
Off-boarding Merchant by
Providing/accecpting notice as per agreement
Recover data/material, if any
Hold sufficient money to process disputes

3. Merchant Lifecycle Framework

3.1 Merchant Onboarding Process

The merchant onboarding process involves several key steps to ensure compliance and mitigate risks:

- **a) Merchant KYC Procedures:**
  - Verification of KYC documents for both the merchant entity and its authorized signatories.
  - Anti-Money Laundering (AML) and due diligence checks are performed for the authorized signatories who have signed the agreement.
- **b) Merchant Screening and Business Validation:**
  - Conducting background and antecedent checks, including screening and business verification.
- **c) Merchant Risk Profiling:**
  - Categorizing risk based on business type, transaction volume, products/services, and historical performance.
- **d) Security Assessment:**
  - Evaluating merchants' adherence to data security and PCI DSS guidelines.
- **e) Record Management:**
  - Maintaining detailed records of KYC, AML validations, and transaction history.
- **f) Transaction Monitoring:**

- Continuous monitoring of transactions for suspicious activity.

- **g) Periodic Due Diligence:**
  - Scheduled reviews to ensure merchants remain compliant with policies.
- **h) Merchant Offboarding:**
  - Defined procedures for offboarding merchants or withdrawing services from non-compliant or high-risk merchants.

3.2 Merchant KYC Procedures: Detailed Guidelines

In accordance with the Reserve Bank of India (RBI) guidelines on Regulation of Payment Aggregators and Payment Gateways (RBI/2020-21/117 CO.DPSS.POLC.No.S33/02-14-008/2020-2021), specifically for onboarded merchants who already possess a bank account utilized for transaction settlement, the requirement to carry out the entire process of KYC (in accordance with the comprehensive KYC guidelines of the Department of Regulation, RBI) may not be applicable.

- **Confirmation of Bank Account:** Verify the merchant's bank account details during onboarding to ensure proper KYC is in place.
- **Adherence to Applicable Guidelines:** We ensure our process for onboarding regulated entities remains compliant with all prevailing RBI guidelines and other relevant statutory regulations governing payment aggregators.

This streamlined approach facilitates efficient onboarding of entities already subjected to stringent regulatory oversight while ensuring adherence to the spirit of Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).

The Reserve Bank of India’s (RBI) Prevention of Money Laundering Act (PMLA), 2002 defines the objective of KYC/AML/CFT (Know Your Customer, Anti-Money Laundering, Combating of Financing of Terrorism) to prevent Banks/Payment Aggregators from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable us to better know and understand customers and their financial dealings, which in turn helps CAMSPay and the Acquiring/Sponsor banks manage their risks prudently.

Merchant KYC is based on the type of entity we onboard, requiring documents such as PAN, Board Resolution, Address proof, and GST, along with other documents for proper due diligence. Refer to **Annexure: I** for an exhaustive list of documents for verification.

A) Customer Acceptance Policy (CAP)

CAP lays down explicit criteria for the acceptance of Merchants. The guidelines for merchant relationships with CAMSPay broadly include the following:

- i. No account-based business relationship will be established in an anonymous or fictitious/benami name.
- ii. Merchants will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done before onboarding to ensure that the identity of the merchant does not match with any person with a known criminal

background or with banned entities, or any individual connected with terrorists or terrorist activities.

- iii. CAMSPay will refrain from entering a business relationship where the identity of the account holder cannot be verified and/or documents/information required cannot be obtained as per the risk categorization, due to non-cooperation of the merchant or non-reliability of the data/information furnished by the merchant to CAMSPay.
- iv. All documents and/or information collected for different categories of merchants will comply with the internal policies/rules of CAMSPay.
- v. A suitable system is in place to ensure that the identity of the merchant does not match with any person or entity whose name appears in sanctions lists/PEP/Blacklists. Any exceptions will be handled on a case-to-case basis with business justification.
- vi. Where Permanent Account Number (PAN) is obtained, it shall be verified from the verification facility of the issuing authority.
- vii. Mandatory documents/information shall be sought at the time of onboarding the merchant and during periodic review. Any additional document shall be obtained only with the explicit consent of the merchant.
- viii. If any suspicion of money laundering or terrorist financing arises during the Customer Due Diligence (CDD) process and performing the CDD could alert the merchant (tipping off), we shall not pursue the process. Instead, a Suspicious Transaction Report (STR) shall be filed with the FIU-IND to address the concerns appropriately.

B) Customer Identification Procedure (CIP)

CAMSPay shall obtain sufficient information necessary to verify the identity of each new customer. CAMSPay shall undertake identification of its merchants during the following stages:

- i. Commencement of an account-based relationship with the merchant.
- ii. When there is a doubt about the authenticity or adequacy of the merchant identification data it has obtained.
- iii. For selling third-party products as agents, selling their own products, payment of credit card dues/sale and reloading of prepaid/travel cards, and any other product for more than rupees fifty thousand.

C) Merchant Screening and Business Validation Process

We conduct background and antecedent checks, and the merchant screening process is carried out based on the documents shared by merchants. The purpose is to verify the nature and bona fides of a merchant's business and conduct a wide range of other checks such as licensing/registration. All documents of high and medium-risk merchants will be reviewed periodically by the Risk team along with other publicly available information.

The business validation process includes validating the merchant's online presence (website/mobile application), products/services sold on the website/app, pricing, contact information, Terms &

Conditions, Refund Policy, PCI DSS, and security-related checks to ensure the merchant follows best practices for accepting secure payments.

D) Merchant Risk Profiling Process

Based on the merchant's business category, products/services, vintage, and bank and network policies, we classify merchants as low/medium/high risk. The risk team reviews each merchant, performs the required level of due diligence, and assigns an appropriate risk level (Low/Medium/High/Critical). Periodic review and other monitoring will be set at this level. Refer to **Annexure: II**.

---

4. Ongoing Due Diligence (ODD)

Ongoing due diligence checks assist CAMSPay in improving its defences against financial crimes such as terrorist funding and money laundering. CAMSPay shall monitor the following types of activities on an ongoing basis:

- i. Suspicious transactions exhibiting inconsistent patterns of transactions such as a spike in velocity, high volume, exceeding thresholds, etc.
- ii. A sudden surge in transactions by a Merchant to a particular entity.
- iii. Fraud reporting cases or any non-compliance in terms of information sharing.
- iv. Merchants identified as high-risk merchants will be reviewed once every six months.
- v. Updates / Periodic updates of KYC shall be carried out at least once every two years for high-risk merchants, once every eight years for medium-risk merchants, and once every ten years for low-risk merchants from the date of account opening / last KYC update.

---

5. Transaction Monitoring & Fraud Risk Management (FRM)

A vital checkpoint post-onboarding is monitoring merchant transactions to identify any variations in transaction volume, chargebacks, frauds, refunds, and direct payer complaints. These variations are key indicators of risk, and the risk team notifies the respective team to take required actions to mitigate impacts on our business.

FRM Process:

As part of the onboarding process, each merchant is mapped to a tailored risk engine configuration within the FRM transaction monitoring system. This engine applies business-specific rule sets and thresholds, drawing on factors such as:

- Historical transactional behaviour
- Pattern deviations
- Merchant category risk exposure
- Negative history/blacklists

These configurations ensure real-time and periodic analysis of transactions to flag anomalies for further investigation.

5.1 Fraud Risk Monitoring Framework

1. Risk Identification

- Monitor transactions for patterns inconsistent with known merchant behaviour.
- Use automated rule-based detection through the FRM application.
- Identify early warning signals to detect potentially fraudulent activity.

2. Risk Assessment

- Classify identified risks by likelihood and impact (low, medium, high).
- Prioritize high-risk patterns or transactions for immediate scrutiny.

3. Detection Mechanisms

- Employ real-time monitoring systems with configurable rules to identify suspicious activities.
- Regularly update rules based on evolving fraud trends, merchant segments, and transaction behaviours.

4. Investigation & Analysis

- Investigate high and medium-risk alerts by designated levels (L1 and L2 reviewers).
- Gather data, perform forensic analysis, and determine whether transactions are suspicious or unauthorized.
- Maintain clear escalation protocols for deeper internal or regulatory investigations.

5. Reporting & Documentation

- All suspicious activity findings are documented, timestamped, and stored securely.
- Confirmed suspicious transactions are escalated to the Compliance Officer and Operations Head.
- Mandatory reporting to FIU must be done within 7 calendar days of identification, as per regulatory guidelines.
- Merchants are not to be informed directly regarding any suspicious transaction reports filed with the FIU.

6. Mitigation & Prevention

- Apply immediate corrective actions to prevent recurring fraudulent behaviour.
- Adjust rules and thresholds for the concerned merchant or segment.
- Update merchant risk category, trigger enhanced due diligence or consider suspension where necessary.

7. Continuous Monitoring & Review

- Periodically review system configurations, alert mechanisms, and rule thresholds.
- Conduct bi-annual audits and evaluations of the FRM process.
- Update internal SOPs in accordance with regulatory changes, emerging fraud patterns, or internal review findings.

5.2 Governance and Review

- This FRM policy note must be reviewed every six (6) months by the Fraud Risk Management team.
- Any updates, including new fraud typologies or revised rules, must be approved by the Operations Head and documented.
- The Compliance team is responsible for ensuring alignment with FIU reporting standards and other regulatory requirements.

---

6. Security Assessment

We follow best practices and guidelines provided by Banks, Networks, PSPs, regulators, and CAMS ISMS to assess the secure integration of merchants. The UAT sign-off team records evidence to ensure merchants use CAMSPay-issued credentials.

6.1 Requirements for Security Audit

CAMSPay performs the activities below to ensure the merchant connects securely to our platform. The merchant needs to implement checks to avoid tampering during the security audit phase as mentioned in **Annexure: III**.

I.1) Request Tampering:

- **Merchant Website -> Request Parameters -> Payment Gateway.**
- The key parameter for online transactions is the amount. If the amount is just passed to the PA without any validation check, it is likely to be exploited. To prevent this, the amount and other relevant parameters (product quantity, check-in/check-out dates, etc.) should be fetched directly from the database to be passed to the PA. If this is not feasible, validating the amount value with any other parameter (i.e., track ID, session variable) would be secure.
- Request amount and response amount should be validated along with the order ID/track ID. If both amounts match, a success message should be displayed on the final page.
- If both amounts do not match, a failure message will be displayed on the final page.

I.2) Response Tampering:

- **Payment Gateway -> Response from PG to Merchant site -> Final Page (Receipt)**

- If it is a hashing model, Hash validation is implemented at our end to avoid response tampering.
- Alternatively, in a normal case, the PG response needs to be stored in the database, and while showing on the final page, data should be fetched from the database based on the track ID.

I.3) URL Redirection Validation:

- Generate a transaction based on the received parameters rather than validating the path it has been posted to. An attacker could redirect the request from failure to success where the response is posted to the relevant page/file and a receipt is generated.

I.4) Duplicate Entry Validation:

- The received transaction details should be validated with already stored database values to verify whether the entry is unique or duplicate. The duplication check should be implemented for unique values (transaction reference ID, Order ID, etc., which are unique for each transaction).

I.5) Receipt Generation:

- Most merchants generate a receipt or store a successful transaction by just checking the response code or message received from the PG rather than other parameters (such as transaction reference ID, Order ID, etc.) of any previous transaction. The receipt should be generated for a transaction if the received response contains all relevant parameters that belong to that transaction.

I.6) Implementation of a Valid and Secure SSL:

- In the TranPortal model where card details are captured at the merchant page, it is necessary to implement a valid, strong SSL certificate to ensure the transaction flow is secure. To know more about the strength of the SSL certificate, scanning it using SSLLABS.COM would provide complete details about the changes that need to be taken care of.

I.7) Secure Sensitive Information:

- In the TranPortal model where card details are captured at the merchant page, card details should not be transmitted in plain text, and details should be securely hashed and transmitted to CAMSPay.
- As per PCI-DSS requirements, card details should not be transmitted in plain text format in a public or shared network. The merchant should add random salt or hash to the card details with salt from the browser before posting it.

I.8) Go-Live:

- The merchant should pass all the above tests to enable CAMSPay payment services, and all the above processes have sufficient audit trails to address any post-facto investigations.

7. Merchant Off-boarding

As per the terms, CAMSPay or its Merchant may terminate the services with an agreed notice period. Upon this activity, CAMSPay will follow the process below:

- Recover all documents/data/materials and any other belongings related to CAMSPay.
- CAMSPay will hold 1% of the gross sale amount in a month to support chargeback and refund claims for the next 6 months. CAMSPay will release the hold after 6 months (The percentage of the hold may change based on the merchant's past chargeback ratio).
- CAMSPay will issue the merchant account closure notification to the merchant.
- Deactivate MID/Utility and other merchant credentials at Acquiring/Sponsor Banks.

I) <u>Annexure: I</u>

Entity Type	**Documents Required**	**Remarks**
Public/Private Ltd	1. Memorandum / Articles of Association and Certificate of Incorporation. 2. Board Resolution / Declaration from company secretary 3. Company PAN and GST 4. Authorized signatory KYC 5. Regulatory/Affiliation certification – If apply	• MOA/AOA should have product/services details • Business category specific certification -e.g., Mutual Fund segment – SEBI Certificate; NBFC – RBI Certificate; Insurance – IRDA Certificate to be collected and verified.
Sole Proprietor	1. Registration certificate (in the case of a registered concern) 2. Certificate / license issued by the Municipal authorities under Shop & Establishment Act (if applicable) 3. Proprietor PAN 4. Certificate / registration document issued under GST / Professional Tax authorities	Registration certificate should have product/services with business address
Partnership/ LLP	1. Certificate of registration (for registered partnership firms only) 2. Copy of partnership deed 3. Copy of Pan Card of Partnership Firm 4. Board Resolution if	Partnership deed should have all the products/services with all the partners name

	LLP	
Govt/Trust/NGO/Society/Education Institution	1. Trust/Society Deed 2. Govt Certificate – if Govt 3. List of Trustees/ members 4. PAN copy 5. Trust Resolution 6. Auth Signatories KYC 7. License as applicable	Deed should have list of products/services

II) Annexure: III

Sr No	Key Points	Status (Yes / No)	Expected Response
1	Unique Merchant Track ID generation-Unique Merchant Track ID should be generated.	(Yes / No)	Yes
2	Request Tampering-Fetching the amount values from the database or passing/validating the required parameters through session/validation parameter (Hash, Encryption, track Id)	(Yes / No)	Yes
3	Response Tampering- Hash validation	(Yes / No/NA)	Yes
4	URL redirection validation	(Yes / No)	Yes
5	Duplicate entry validation	(Yes / No)	Yes
6	Receipt Generation	(Yes / No)	Yes
7	Implementation of a valid and secure SSL (for TranPortal integration)	(Yes / No)	Yes
8	Secure Sensitive information (Card info, CVV etc.) for TranPortal Integration	(Yes/ No)	Yes