Merchant On-boarding Policy

Computer Age Management Services Limited

For its Payments Business (CAMSPay)

Confidential

Version – 1.5

Introduction

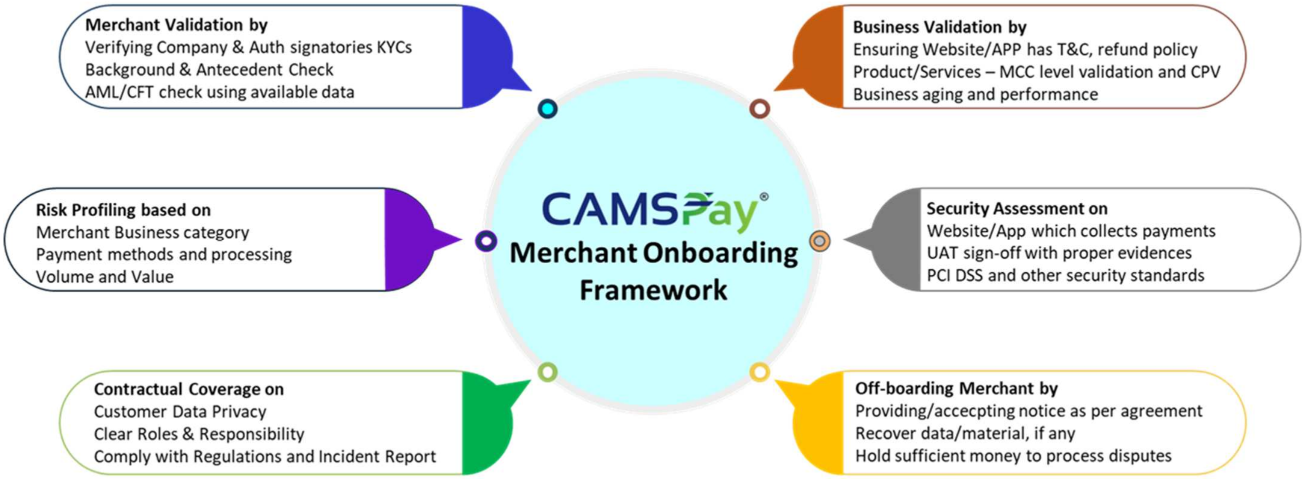
CAMSPay – a Strategic Business Unit of Computer Age Management Services Ltd focused on Payment aggregation, regards and treats Merchant Onboarding as a critical activity of its Business operations. This Merchant onboarding policy document defines the process to onboard merchants effectively with required controls in place.

Merchant Onboarding Policy

As a Payment Aggregator, while onboarding merchants, CAMSPay conducts KYC based on nature of business, Business validation including products/ services sold on their website/app and whether the website and Mobile application have required Terms and Conditions and other polices as required. The onboarding covers due diligence checks, Risk profiling based on business and product category, business background & antecedent check, transaction monitoring, ongoing due diligence, and periodic updates to ensure merchants do not have any malafide intention of duping customers do not sell fake/counterfeit/prohibited products using CAMSPay platform.

CAMSPay's Merchant onboarding process defines the process to evaluate a merchant as per extant KYC rules and guidelines issued by Banks and regulators by time to time which are applicable to the Merchant business category, screening the risk of the merchants based on the business category, determine whether to onboard a merchant and onboard qualified merchants smoothly.

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

Merchant Onboarding Process

The onboarding process designed for effective and seamless collaboration and coordination between multiple teams and each stakeholder will have their process with a clear SOP and TAT. The below process supports us to comply with regulation and to mitigate the risks.

1. Merchant KYC Procedures
2. Merchant Screening and Business Validation Process
3. Merchant Risk Profiling Process
4. Record Management Process
5. Transaction Monitoring
6. Periodic due diligence and update
7. Security Assessment
8. Merchant Off-boarding

1. Merchant KYC Procedures

Reserve Bank of India's (RBI) **Prevention of Money Laundering Act, (PMLA), 2002** defines the objective of KYC/AML/CFT (Know Your Customers, 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 to know/understand customers and their financial dealings better which in turn helps CAMSPay and the Acquiring / Sponsor banks manage their risks prudently.

Merchant KYC based on the type of entity we onboard including PAN, Board Resolution, Address proof, GST, verify beneficial ownership using shareholders and directors list with other documents for proper due diligence. Refer the below exhaustive list of documents for verification.

Entity Type	Documents Required	Remarks
Public/Private Ltd	1. Memorandum / Articles of Association and Certificate of Incorporation. 2. Board Resolution 3. Company PAN and GST 4. List Of Directors 5. Authorized signatory KYC 6. 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 3. CST / VAT certificate 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 LLP	Partnership deed should have all the products/services with all the partners name
Govt/Trust/NGO/Society	1. Trust/Society Deed 2. Govt Certificate – if Govt 3. List of Trustees/ members 4. PAN copy 5. Trust Resolution 6. Auth Signatories KYC	Deed should have list of products/services

2. Merchant Screening and Business Validation Process

Next, we conduct a background and antecedent checks, and the merchant screening process will be carried out based on the documents shared by merchants. The purpose is to verify the nature, bona fides of a merchant business and wide range of other checks such as licensing/registration, credit, Profit and Loss checks and balance sheet review etc. and all the documents will be reviewed periodically by Risk team along with other publicly available information.

Business Validation – Merchant online presence validation including Website/Mobile application, product/services sold on the website/app, pricing, contact information, Terms& Conditions, Refund Policy, PCI DSS, and security related checks will be performed to ensure merchant follows best practices for accepting secure payments.

3. Merchant Risk Profiling Process

Based on the Merchants business category, product/services, vintage, banks, and network policy we classify merchants as low/medium/high risk. Risk team reviews each merchant and performs required level of due diligence and assigns an appropriate risk level like Low/Medium/High/Critical. The periodic review and other monitoring will be set at this level.

4. Record Management Process

All merchant related documents including KYC, Website information, risk assessments, transaction and other related information are stored perform periodic internal risk review and governance. The process will be managed by CAMSPay compliance officer, and the data will be stored as per Document Storage Policy.

5. Transaction Monitoring

A vital check point 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 risk team notifies the respective team to take required actions to not impact our business.

6. Periodic due diligence and update

Ongoing due diligence checks highlight any change in merchant websites, products/services will lead to risk profile change. The frequent update on these things including company details like contact personnel changes etc needs to be updated regularly and risk management team will raise it as early warning signal if any variations.

7. Security Assessment

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

7.1 Requirements for Security Audit

CAMSPay performs the below activities to ensure merchant connects securely to our platform. The merchant needs to implement the below checks to avoid tampering in the security audit phase.

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**

7.2 Request Tampering:

Merchant Website -> Request Parameters -> Payment Gateway.

The key parameter for online transactions is the Amount. If the amount is just passing to the PA without any validation check, then it is likely to get 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 it is not feasible then 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 order id/track id, if both amounts are getting matched then success message should be displayed on the final page.

If both amounts are not getting matched, then failure message gets displayed on the final page.

7.3 Response Tampering:

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

If it is a hashing model, then Hash validation is implemented at our end to avoid response tampering.

Or

In normal case, PG response needs to be stored in the database and while showing on the final page fetch the data from the database based on track ID.

7.4 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.php to success.php where the response is posted to the relevant page/file and receipt is generated.

7.5 Duplicate entry validation:

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

7.6 Receipt Generation:

Most of the merchants generate the receipt or store a successful transaction by just checking the response code or message that has been 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.

7.8 Implementation of a valid and secure SSL:

In the TranPortal model where the card details are being 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 give complete details about the changes that need to be taken care of.

7.9 Secure Sensitive information:

In the TranPortal model where the card details are being captured at the merchant page, Card details should not go in plain text, and details should be securely hashed and transmitted to CAMSPay.

As per the PCI-DSS requirements, the card details should not be transmitted in plain text format in the public or shared network. The merchant should add random salt or hash to the card details with salt from the browser before posting it.

7.10 Go-Live

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

8. 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 below process.

- 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 % of the hold may change based on merchants 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

VERSION HISTORY & CONTROL

Version	Date	Prepared by	Approved by	Change History
1.2	13/08/2021	Prabakaran Palani	Vasanth J E	Initial document
1.3	14/09/2021	Prabakaran Palani	Vasanth J E	Updated Merchant Off-boarding Process approved by Board on 14/09/2021
1.4	29/07/2022	Prabakaran Palani	Vasanth J E	Updated Onboarding Life cycle
1.5	26/07/2023	Prabakaran Palani	Vasanth J E	Reviewed & no change