HITACHI
Inspire the Next

Merchant Onboarding Policy

Date	Version	Description	Approved By
28/10/2021	1.0	Original Document	Board of Directors
20/02/2023	1.1	Document Review	Managing Director
15/01/2024	1.2	Document Review	Managing Director

Table of Contents

HITACHI
Inspire the Next

1. Introduction

1.1 Hitachi Payment Services Pvt Ltd (HPY) PA (hereinafter referred to as the "company"), seeks to document the practices and procedures to be followed by the company for acquisition of new Merchants. The company believes in human centric innovation and customer is at the core of their business. To offer a faster, secure and seamless onboarding experience, HPY PA has detailed this Merchant Onboarding Policy.

1.2 Reserve Bank of India ("RBI") vide its Guidelines on Regulation of Payment Aggregators(PA) and Payment Gateways dated 17 March 2020, as amended or clarified from time to time ("PA Guidelines") has mandated payment aggregators to have a board approved Merchant Onboarding Policy.

1.3 The Merchant Onboarding Policy is required to amongst others lay down guiding principles for onboarding of Merchants in accordance with the requirements specified by the PA Guidelines and other applicable regulations such as RBI Mater Directions- Know your Customer Directions, 2016, as amended or clarified from time to time ("KYC Master Directions").

2. Objective of the Policy

The following are the objectives of this merchant onboarding policy of HPY PA:

i. Define a seamless and efficient process for onboarding Merchants through digital channels and Fleet on Street (FOS). The same shall include merchant evaluation and assessment, merchant segmentation, merchant onboarding, etc.
ii. Facilitate the merchant acquisition process which includes activities such as agreement preparation, merchant due diligence, documentation verification, risk categorization, activation and maintenance of merchants etc.
iii. Define ongoing merchant monitoring measures to be undertaken
iv. Establish the guidelines for the company to take steps in case it decides to discontinue its relationship with the merchant or delist the merchant

3. Scope and Applicability

This policy shall be applicable to all the merchants with whom the company establishes a relationship. It is also applicable to the FOS and Backend Operations team members (Merchant Onboarding Support, Senior Manager- Merchant On boarding, VP Operations) in the company who are responsible for the merchant acquisition/onboarding functions.

4. Channels of Onboarding

Lead generation and Merchant sign-up would be possible through various online digital channels like website, Merchant mobile application, etc. Digital on-boarding of the merchant would be done by FOS.

5. Roles and Responsibilities

FOS shall be responsible for signing up the Merchant, uploading and verifying of Merchant KYC documents & bank account, submission of documents on Mobile Application. The Backend Operations Team shall be responsible for authenticating the Merchant. Operations VP shall monitor the onboarding process.

6. Key Features of Onboarding

i. Real-time onboarding of merchants
ii. Digital verification of KYC documents
iii. Complete visibility and real-time tracking of applications
iv. Digital process eliminating the need of physical forms, IDs and documents
v. OCR feature for fetching details from ID cards thereby minimizing human errors
vi. Digital process leading to faster onboarding, verification and customer delight.
vii. Transparency in the process

7. Merchant Onboarding Procedure

As per the RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways and Master Direction on Know Your Customer (KYC), 2016, the company shall undertake Merchant assessment to comply with the regulatory requirements and as a preventive measure against the risks involved in the approval of the new Merchants.

Below given is the process followed by the company for onboarding Merchants:

7.1 Merchant sign up and authentication:

i. An android mobile application will be provided to the FOS to digitally onboard Merchants. This application will allow FOS to fill basic details of the merchant, capture image & upload personal & business ID proofs, capture bank account details, E-sign contracts, etc.
ii. The FOS shall visit the merchant location and collect documents as mentioned under Appendix I. For OVDs, details are extracted from the respective authorized databases and auto populated onto the application.
iii. Details of the entity including CIN are fetched from the respective registrar database and verified.
iv. The OVDs and other IDs are verified by using proprietary AI based pattern level check algorithms and raises a red flag if wrong image or junk image was captured by the FOS.
v. The Forgery Engine of the application ensures that no photocopies or Xerox images are uploaded and ensures compliance with regulations
vi. Forgery Engine of the app has the capability of extracting face from ID cards and ability to match them with each other.
vii. Merchant bank account is validated via Penny drop.

7.2 Additional Details captured:

i. Photo of the premises
ii. Nature of Business
iii. Daily transaction limit

iv. Average monthly business volume of the Merchant
v. Details of commercials/fees – Merchant Discount Rate (MDR), Rental, commitment charges, etc.

7.3 Merchant background check:

i. Background screening is done at this stage for the purpose of verification of the authenticity of the Merchant's intentions, business model, and purpose.
ii. Necessary assessment shall be done to ensure that Merchants onboarded are not potential fraudsters or shell companies and that they do not sell fake/ prohibited/ counterfeit products, etc.
iii. Credit worthiness of the business and/or its owners shall be evaluated by doing credit bureau checks.
iv. The company shall analyse and review Merchant's web presence and content i.e. affiliated press articles, domain name, social media pages and online Customer ratings to build a full profile of the Merchant and their reputation.
v. The company shall also verify if the Merchant's website clearly indicates the product/service offered, mandatory parameters (About Us, Privacy Policy, Contact Us, Product Checkout), terms and conditions and timeline for processing returns and refunds.
vi. The company shall also scrutinize the business, track record, verify commercial history, etc.
vii. Name screening shall be done against negative/sanctions list published by United Nations Security Council.

7.4 Merchant Risk Profile/Risk Categorization:

Merchants shall be categorized as low, medium or high-risk which in turn will determine the level of scrutiny applicable. Risk rating will be based on due diligence factors such as Merchant's longevity, financial stability, industry, business model, products sold / services offered, and previous processing history, etc.
Refer to Section 5 : Risk Categorization (KYC AML Policy) for further details.

7.5 Security Assessment:

The Merchant will be expected to comply with applicable law related to security of personal data. A review will be conducted at periodically in order to ensure compliance with regulatory security standard benchmarks.
Refer to Section 9: Security Risk Assessment for further details.

7.6 Merchant Agreement:

i. On successful submission of the application by the FOS, the Merchant agreement is generated.
ii. A digital form with all the Merchant details is shared with the Merchant. This form will also show the predefined charges & rates based on the type of product/service opted for by the merchant.
iii. The agreement is then physically signed and stamped by the Merchant
iv. The agreement is then franked as per the prevalent stamp duty of the respective state
v. Post this, the agreement is scanned and uploaded on the Application.

7.7 Scrutiny of Merchant Application:

i. Back Operations Team reviews the merchant application, details of the ID proof, risk flags as submitted by the FOS on the Mobile Application.
ii. The application submitted by FOS through the onboarding application will be approved/rejected/ sent for rework to the respective FOS by the Back Operations Team.

7.8 Generation of MID/ TID:

i. Post successful onboarding, MID/TID is generated on the Merchant Management System (MMS).
ii. Post generation of MID/ TID,
    - In case of Point of Sale (POS) Terminal, the terminal is installed at the merchant location and a test transaction is conducted by the FOS.
    - In case of online PG, an onboarding kit is shared for web integration, testing of test transaction.

8. Ongoing Monitoring

After onboarding, businesses need to do constant due diligence checks to monitor any changes in merchant behaviour. The backend operations team would monitor the Merchant's activities to ensure they are consistent with their knowledge about the Merchants, Merchants' business, and risk profile and the source of funds. The company shall outline how monitoring will occur, when it will occur, how reviews and feedback are conducted and how risk exposures are identified and mitigated.

Ongoing due diligence checks assist organizations in improving their chances against financial crimes such as terrorist funding and money laundering. The Company shall monitor on an ongoing basis the following types of activities:

i. Suspicious transactions having inconsistent patterns of transactions such as spike in velocity, high volume, exceeding threshold, etc.
ii. 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. Out of area or unusual cross-border activities
v. Stricter monitoring for Merchants identified as high-risk Merchants
vi. Adverse media mentions
vii. Increase in chargeback/return/refund cases
viii. Change in website details or contact information can be a hint of fraud.

9. Security Risk Assessment

RBI Guidelines state that Payment Aggregators should undertake comprehensive security assessment during onboarding process to ensure that minimal baseline security controls are adhered to by the Merchants. The company is exposed to significant cyber risks and compliance liabilities due to its Merchants. For this purpose, the company shall conduct comprehensive security assessments during onboarding to ensure adequate safeguards in place as applicable.

i. HPY PA will undertake comprehensive security assessment during Merchant onboarding process to check compliance to security controls. HPY PA will obtain periodic security assessment reports either based on the risk assessment (large or small Merchants) and / or at the time of renewal of contracts.
ii. HPY PA will check Payment Card Industry-Data Security Standard (PCI-DSS) and Payment Application-Data Security Standard (PA-DSS) compliance of the infrastructure of the Merchants on-boarded as applicable.

iii. A security audit of the Merchant may be carried out to verify that card details are not stored by the Merchant.
iv. Agreements with merchant will include clauses related to security/ privacy of Customer data as well as compliance to PA-DSS and incident reporting obligations.

10. Deactivation of Merchants

Merchant account may be deactivated or otherwise restricted from accessing or using the PA Platform or Services in the event of:

i. Violation of Terms of Use as per the agreement between the company and the Merchant
ii. Disparagement of the company or any of its affiliates
iii. Termination request from the Merchant
iv. High chargebacks and/or substantial fraud transactions on the gateway
v. Complaints against the Merchant

11. Policy Review

The policy is reviewed on an annual basis and updated to incorporate changes as per RBI Guidelines. All updates/changes to the Policy will be communicated to the relevant staff/relevant stakeholders on a periodic basis. All such changes /modifications will be reported to the Board for approval.

12. Record Management

In line with Master Direction – KYC Direction, 2016, HPY PA shall take the following steps for maintaining, preserving and reporting of Customer information:

i. Maintain all necessary records of transactions with Customers including the Merchant agreement, Merchant application, documentation, transaction data, etc. for at least five years from the date of transaction.
ii. Preserve the records pertaining to the identification of the Customers and their addresses obtained while onboarding the customer and during the course of business relationship, for a period of five years from the date of cessation of the transactions.
iii. Make available the identification records and transaction data to the competent authorities upon request.
iv. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
    - the nature of the transactions
    - the amount of the transaction
    - the date on which the transaction was conducted and
    - the parties to the transaction.
v. Evolve a system for proper maintenance and preservation of Customer information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

HITACHI
Inspire the Next

Appendix I - Entity Wise Document List

Particulars	Specific Checks
Individual Checks	
PAN Card / Form 60	• PAN Number is validated by third-party vendor • Collected for Ultimate Beneficial Owner (UBO) and/or Authorised Signatory and/or Power of Attorney and/or Authorisation holder
Officially Valid Document (OVD): (Any 1) Passport, driving license, proof of possession of Aadhaar number, the Voter's Identity Card, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register.	• Aadhaar Card is authenticated via Aadhaar XML • Collected for Ultimate Beneficial Owner (UBO) and/or Authorised Signatory and/or Power of Attorney and/or Authorisation holder • Match all details on OVD with that on PAN (e.g.: name, birthdate, image, etc.)
Individual Address proofs (if required): Utility bills, Property/Municipal Tax receipts, Pension orders and Letter of allotment	• Match name and address with PAN and other documents • Match address proof with details provided during sign-up

Proof of address of foreign nationals: Any document issued by the Government departments of foreign jurisdictions and/or letter issued by the Foreign Embassy or Mission in India.	
Cancelled Cheque	• Bank Account details are verified using Penny Drop
Legal Entity Checks	
Company • Certificate of Incorporation • MoA and AoA • PAN Card • Board Resolution • Ownership Structure and UBO declaration • OVD of Authorised signatory • Cancelled Cheque	• Verify name, CIN/DIN/LLP via MCA Portal • Board Resolution is verified by matching authorised signatory details on AoA, MoA • OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop
Partnership/Limited Liability Partnerships (LLP) • Registration Certificate • PAN • Partnership Deed/LLP agreement • Power of Attorney • OVD of Authorised signatory • Cancelled Cheque	• Registration checks based on available databases • OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop

Sole Proprietorship
• PAN and OVD of proprietor
• Any two of the below documents as proof of business
  ○ Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
  ○ Registration Certificate
  ○ Sales and income tax returns.
  ○ 36CST/VAT/ GST certificate (provisional/final).
  ○ Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
  ○ IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
  ○ Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is
	• OVD of Authorised signatory is verified as mentioned above
	• PAN Number is validated by third-party vendor
	• Registration checks based on available databases
	• Bank Account details are verified using Penny Drop

reflected, duly authenticated/acknowledged by the Income Tax authorities. ○ Utility bills such as electricity, water, landline telephone bills, etc • Cancelled Cheque	
Trusts • Registration Certificate • PAN Card • Trust Deed • Power of Attorney • OVD of Authorised signatory • list of beneficiaries, settlors and trustees • Cancelled Cheque	• Registration checks based on available databases • OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop
Unincorporated Association or a body of individuals • PAN Card • Power of Attorney • Resolution of the managing body • OVD • Cancelled Cheque	• OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Registration checks based on available databases • Bank Account details are verified using Penny Drop
Hindu Undivided Family (HUF) • PAN Card • Resolution of managing body • Power of Attorney • HUF Deed (if applicable) • Cancelled Cheque	• PAN Number of the Company is verified as mentioned above • Registration checks based on available databases • Bank Account details are verified using Penny Drop

HITACHI
Inspire the Next

Appendix II – Prohibited Businesses List

1. Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services
2. Body parts which includes organs or other body parts
3. Child pornography which includes pornographic materials involving minors
4. Drugs and drug paraphernalia which includes hallucinogenic substances, illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms
5. Illegal goods which includes materials, products, or information promoting illegal goods or enabling illegal acts
6. Weapons which includes firearms, ammunition, knives, brass knuckles, gun parts, and other armaments
7. Websites depicting violence and extreme sexual violence
8. Bestiality