- Concerto Systems & Software

Merchant On-Boarding and Compliance

concerto
Payment Systems Architects

Restriction on disclosure

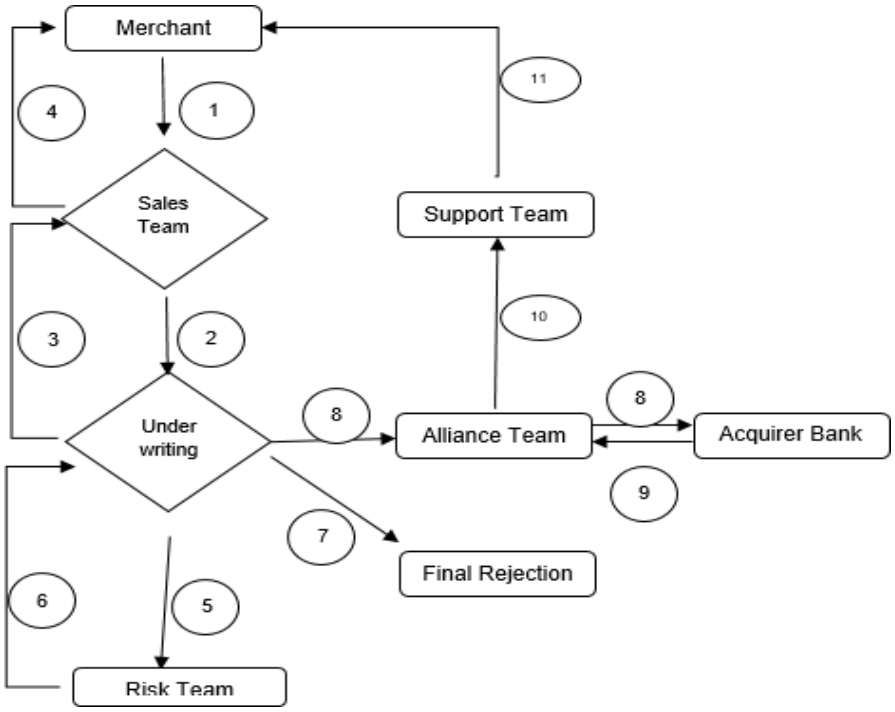
The information (data) contained in this document constitutes confidential information of Concerto Software & Systems Private Limited and is provided for evaluation purposes only. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence. The disclosure of which would provide competitive advantage to others. This document shall not be disclosed, used or duplicated, in whole or in part, for any purpose.

Revision History

Ver. No	Revision Date	Author	Reviewed by	Approved by	Modification Details	Modification on page
1.0	**13 April 2024**	**'Mahabaleshwar Kate**	**Manish Mer**	**Jiss Jose**		
2.0	**29 January 2025**	**'Mahabaleshwar Kate**	**Manish Mer**	**Jiss Jose**	CPV & Aadhaar details	**19 & 9**

Contents

1. Merchant Onboarding Process Flow



Process Flow

1) Merchant Submits KYC to the Sales Team.
2) The Sales Team conducts basic verification of credentials and submits the documents to the Underwriting team.
3) The Underwriting Team runs a Document and Website Verification. In case of discrepancies, the team rejects the application and returns the case to the Sales team.
4) The Sales team addresses the critical discrepancies by collecting additional information from the merchant and re-submits the document to the Underwriting team.
5) The Underwriting team further scrutinises the Documents and Website and upon approval, sends them to the Risk team.
6) The Risk Team visits the Merchant's office and conducts other risk analysis and submits the Reports to the Underwriting team.
7) The Underwriting team either approves or rejects the case based on the reports. If rejected, the case goes back to Sales team for final rejection.
8) The approved case is sent to the Alliance team, which forwards the application to the Acquiring bank.
9) The Acquiring Bank issues the MID and sends it back to the Alliance team.
10) The Alliance team further sends the required details to the support team, which configures the merchant, assisting the merchant with configuration and going live.

2. Sales Process

Process for SMEs and Retail outlets

The Sales Team conducts a sign-up of interested merchant & close on the commercials for the merchant.

At the time of on-boarding, the Sales Team collects all the information required from the Merchant for Sign-up application. This includes details as following:-

- Account Information
- Merchant Code*:
- Mobile Number*:
- Merchant Contact Person*:
- DBA (Brand) Name*:
- Address:
- Location:
- Pin code*:
- City*:
- State*:
- Date of Incorporation:
- Company Total Turnover:
- Online Turnover:
- IP Address for Whitelisting:
- Pan No:
- GSTIN:
- MCC*
- Bank Details
- Beneficiary Name:
- IFSC:
- Account No*:
- Beneficiary Bank Name:
- Merchant Website URL:
    i. Terms and Condition Link
    ii. Product and Pricing link

iii. Refund and Cancellation Link
iv. Contact us Link

- Remark: If any, in case of exception

In merchant sign-up process, Sales team will collect all KYC documents as specified above from the Merchant. The Sales team is responsible to gather as much information as possible from the merchant in order to process the application and to mitigate the risk associated with the merchant. The Merchant needs to be educated with the advantages and risks associated with the ecommerce business. The merchants are further guided to take necessary precautions and security measures so that they can protect themselves from online frauds. The Sales team needs to ensure that the merchant follows all the safety measures and process defined by Concerto Software and Systems Pvt. Ltd. Any suspicious activity done by the merchants needs to be highlighted to the risk team in order to avoid fraudulent transactions.

The Sales team forwards the KYC documents, merchant application form and other information to the underwriting team.

3. KYC Documentation Process

3.1. KYC documents basis of Entity Type

Following is the list of KYC documents required to on-board every merchant. KYC Document Verification on the basis of entity type ensures that all the relevant documents are collected from the Merchant. Ensure that all the KYC documents are all uploaded in Merchant Sign-up process, else the system does not allow merchant account approval. In cases like MOA, AOA or Deeds, heavy documents are likely to be accepted over email. However, prior to merchant approval it is mandatory to have all documents in place.

KYC Document upload	
1	**Merchant identity proof - As applicable (ONE of the following documents is required)**
a)	Partnership firms: Signed and valid Partnership Deed
b)	Trust: Signed and valid trust deed
c)	Society: Signed and valid bye-laws of the society
d)	Sole Proprietorship: PAN number of sole proprietors
e)	Private Limited Company: Copy of MOA/AOA/Certificate of Incorporation
e)	Public Limited Company: Copy of MOA/AOA/Certificate of Incorporation
f)	Board Resolution authorizing the authorized Signatory (if signatory is different from promoter/director/partner/etc.)
2	**Merchant existence proof (ONE of the following documents is required)**
a)	Establishment's PAN
b)	Central Sales Tax Registration Number or Regional Sales Tax Number where applicable
c)	Government issued business license –Trade/Municipal License
d)	Government registration authorizing the Processed Merchant to run the business
e)	For Schools, College establishments – Copy of establishment registration document

f)	Excise Registration Number
g)	Shop & Establishment License Number
h)	Importer Exporter Code
I)	Registration Number issued by Registrar of Firms
j)	Service Tax registration certificate
3	**Business Address Proof (ONE of the following documents is required)**
a)	Utility Bills (Telephone, Electricity bill Not older than 3 months)
b)	Any other Government document clearly showing the address of the company
c)	Rental agreement copy along with utility bill not older than 3 months in the name of the landlord.
5	**Authorized Signatories signature Proof (ONE of the following documents is required)**
a)	Authorized Signatory PAN Copy
b)	Driving License
c)	Passport
6	**Authorized Signatories - Address Proof (ONE of the following documents is required)**
a)	Passport (with Address Page)
b)	Bank Account Statement
c)	Utility Bills (Telephone, Electricity bill Not older than 3 months)
d)	Rental agreement copy along with utility bill not older than 3 months in the name of the landlord.
e)	Aadhaar Card (Masked) with Aadhaar Consent.
7	**Bank Account details proof (ONE of the following documents is needed)**

a)	Cancelled cheque
b)	Bank statement (which clearly mentions account number and IFSC)
8	**TAX Certificate**
a)	GST Certificate
b)	SEZ License Proof
c)	Turnover proof
d)	Govt. issued certificate if any

3.2. Special Doc Requirements for special business

In certain cases where the merchant operates in a highly regulated industry, it is essential to procure additional documentation to establish proof of adherence to regulatory guidelines.

Nature of Business	Document Recommended
Travel Companies/Hotel	IATA Certificate (Compulsory if Air ticket booking) OR
	Registration from Department of Travel & Commerce. OR
	Agreement between third party and Merchant. OR Agreement between Merchant and Hotel company.
Education	CBSE Registration certificate
	Affiliation Certificate
Food Related Business	FSSAI Certificate
Ayurvedic products	AYUSH Certification
Drugs and Pharmacy	Registration with Drugs Controller General of India Stem cell banking companies
Telecom and/or ISP	ISP License
Doctor	Registration Certificate

Broker & Research company	Broker License/SEBI certificate
Insurance	IRDA License
B2B	It must have Agent Login, and a sample login must be provided to check the flow. If this is not possible, a document with detailed screenshots must be provided.
Hotel & Resorts Industry	FHRA

4. Underwriting Process

The Underwriting process is very crucial during Merchant Onboarding. The underwriting team verifies the KYC documents and categorizes the merchants based on the risk associated with the businesses. The Underwriter is also responsible to verify the website content and cross check it with the details available in the application.

4.1. Merchant Risk Level

Risk levels 1 and 5 indicate the lowest and highest levels of risk respectively. Broad guidelines for setting appropriate risk levels are below (detailed guidelines are available in the Merchant Onboarding screen, under the “risk & compliance” section. Setting the appropriate risk level is very important because certain back-end rules (like blacklist rules, velocity rules, etc.) are set in the database depending on the chosen risk level. Choosing an overtly permissive risk level exposes to fraud and misuse whereas choosing an overtly restrictive risk level exposes to delayed processing and false positives.

Below are the defined risk levels for various types of merchants:

Risk Level 1: Educational institutions, schools, colleges and membership fees for renowned associations and statutory bodies.

Risk Level 2: Broadband and internet services with recurring monthly post-paid payment and other similar services which are recurring payments on a post-paid basis. Other low ticket size ecommerce payments (such as movie ticket purchases) also fall under this risk level. Utility billers (direct billers like Vodafone, Tata Sky, etc.) also fall under this risk level but please note, utility bill payments through bill aggregators will fall under risk level 3 and NOT this level.

Risk Level 3: E-commerce merchants accepting domestic payments and only doing domestic delivery (to domestic PIN codes) also fall under this risk level. Any ecommerce business which has average ticket size greater than 4-5000 will fall in this bucket. Travel merchants who accept only domestic payments (from cards issued in India) also fall under this bucket. Recharge (phone, DTH, etc.) and utility payments via third party bill payment aggregators. Special note: It has been observed in many instances that the third-party bill aggregators use a “wallet mechanism” to store user money and allow for utility payments from that stored money. In such cases, those merchants will fall under risk level 4 since the option of money storage hugely increases the chances of risk.

Risk Level 4: Any merchant who intends to use international payments automatically falls in risk level 4, irrespective of their line of business. For example, even an educational institution which would normally fall under risk level 1 is automatically demoted to risk level 4 if they opt for international payments. Any and all PPIs (Prepaid Instruments) i.e. wallets who use the PG for wallet loading also fall in risk level 4 Special note: RBI regulations on wallets are very clear in terms of usage of the money stored in a wallet. However, there are cases where some merchants offer utility payments via “wallets”. This case falls under a grey area on whether it should be considered a closed or a semi-closed wallet (requiring RBI licensing). On one hand, payment is being made to external entities (like Mahanagar Gas, Airtel, Jio, etc.) and on the other,the ‘inventory’ has been purchased beforehand by the aggregator and therefore wallet money is being used for purchase on the same website/entity and not different legal entity. Nevertheless, any merchant who has a business model of “stored money” should be treated as a risk level 4 merchant.

Risk Level 5: High risk categories such as resume writing, job/employment services, matrimonial, ecommerce websites without a proper web presence from known high risk regions, freelancers, medicine & pills, dating websites or apps. As a company strategy, we typically do not prefer to work with such merchants. In case the sales team is convinced of the viability of a merchant who falls in the risk level 5 bucket, kindly put up an email request to assess the merchant. It should be noted that most of our acquirers do not accept such merchants and we might have to specifically work with our acquirers on a case-by-case basis in case such merchants are being on boarded. Note: Risk level 5 merchants cannot be on boarded without “buyer protection” being turned on.

4.2. Merchant website analysis

Prior to go-live, the merchant’s website needs to be scanned for several points which are outlined below :

4.2.1. Complete description of goods and services

By definition, a merchant intending to collect online payments has to be selling something – a certain good or service. This has to be clearly reflected on the merchant website.

The Merchant must provide a complete description of its goods or services. This is easy in the ecommerce context. In other cases (like educational institutions etc. where a standard “set of products” cannot be displayed), the website should at least provide descriptions of the kind of services being offered.

In general, the sales and risk personnel, both, must be absolutely aware of:

- WHAT is being sold
- TO WHOM it is being sold
- HOW will the sold product/service be delivered to the customer
- WHEN will the sold product/service be delivered to the customer
- IN WHAT FORM will the sold product/service be delivered to the customer

4.2.2. Merchant Contact Information

Since communication with a Merchant is not always possible using the Website, Merchants must display a Customer service contact telephone number or e-mail address. The Customers can, therefore, contact the Merchant to ask questions about their transaction.

It is necessary to attempt to contact the merchant on this provided contact information at least once during the on boarding or post-on boarding process to ensure legitimacy of the contact information.

4.2.3. Return, Refund and Cancellation Policy

A Merchant must provide sufficient details of their return, refund, and cancellation policy clearly on the Website to inform customers of their rights and responsibilities, for example, in case they need to return goods. It is perfectly acceptable if the Merchant has a limited or no refund policy, but this must be very clearly communicated to customers before the purchase decision is made, to prevent misunderstanding and disputes.

4.2.4. Delivery Policy

In the event that any merchant is unable to support delivery of goods worldwide and restricts sales to within their own country or to a limited number of countries, based on delivery experience or import and export regulations, the same shall be communicated on the website explicitly stating the countries and regions where delivery of goods can be made.

It is also recommended to clearly state the delivery timeframe or at least indicative delivery timeframes. It is recommended to provide details of the course of action in case delivery timeframe is overshot.

4.2.5. Transaction currency and currencies

In case of merchants who are utilizing MCC and/or overseas card acceptance, it is understood that since the merchant's customer base is worldwide, it is important that the customer is made aware of the transaction currency before the Customer proceeds to purchase. The currency should be clearly stated, including the country name when the name of the unit of currency is not unique. For example, a dollar can be an Australian dollar, a New Zealand dollar, a Hong Kong dollar, a U.S. dollar and so on.

4.2.6. Additional items that ideally should be included on a merchant's website

- Privacy statements
- Identifiers that easily match the Website to the trade name of the Merchant
- A statement encouraging Customers to retain a copy of the transaction record in email and/or SMS, etc.

4.3. Banned and Prohibited categories

The following list is a set of prohibited categories which none of our acquirers would accept processing for. For reference the complete list has been reproduced below :

a. Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services.

b. Alcohol or alcoholic beverages such as beer, liquor, wine, or champagne.

c. Body parts which include organs or other body parts.

d. Bulk marketing tools, which include email lists, software, or other products enabling unsolicited email messages (spam).

e. Cable descramblers and black boxes which include devices intended to obtain cable and satellite signals for free.

f. Child pornography which includes pornographic materials involving minors.

g. Copyright unlocking devices which include Mod chips or other devices designed to circumvent copyright protection.

h. Copyrighted media which includes unauthorized copies of books, music, movies, and other licensed or protected materials.

i. Copyrighted software which includes unauthorized copies of software, video games and other licensed or protected materials, including OEM or bundled software.

j. Counterfeit and unauthorized goods which include replicas or imitations of designer goods; items without a celebrity endorsement that would normally require such an association, fake autographs, counterfeit stamps, and other potentially unauthorized goods.

k. Drugs and drug paraphernalia which include illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms.

l. Drug test circumvention aids which include drug cleansing shakes, urine test additives, and related items.

m. Endangered species which includes plants, animals or other organisms (including product derivatives) in danger of extinction.

n. Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, and related content.

o. Government IDs or documents which includes fake IDs, passports, diplomas, and noble titles.

p. Hacking and cracking materials which include manuals, how-to guides, information, or equipment enabling illegal access to software, servers, watomites, or other protected property.

q. Illegal goods which include materials, products, or information promoting illegal goods or enabling illegal acts.

r. Miracle cures which include unsubstantiated cures, remedies or other items marketed as quick health fixes.

s. Offensive goods which include literature, products or other materials that: a) Defame or slander any person or groups of people based on race, ethnicity, national origin, religion, sex, or other factors b) Encourage or incite violent acts; and/or c) Promote intolerance or hatred.

t. Offensive goods, crime which includes crime scene photos or items, such as personal belongings, associated with criminals.

u. Prescription drugs or herbal drugs or any kind of online pharmacies which includes drugs or other products requiring a prescription by a licensed medical practitioner.

v. Pyrotechnic devices and hazardous materials which includes fireworks and related goods; toxic, flammable, and radioactive materials and substances.

w. Regulated goods which include air bags; batteries containing mercury; Freon or similar substances/refrigerants, chemical/industrial solvents, government uniforms, car titles or logos, license plates, police badges and law enforcement equipment, lock-picking devices, pesticides; postage meters, recalled items, slot machines, surveillance equipment; goods regulated by government or other agency specifications.

x. Securities, which include stocks, bonds, or related financial products.

y. Tobacco and cigarettes which includes cigarettes, cigars, chewing tobacco, and related products.

z. Traffic devices which include radar detectors/ jammers, license plate covers, traffic signal changers, and related products.

i. Weapons which include firearms, ammunition, knives, brass knuckles, gun parts, and other armaments.

ii. Wholesale currency which includes discounted currencies or currency exchanges. cc. Live animals or hides/skins/teeth, nails and other parts etc. of animals.

iii. Multi-Level Marketing collection fees

iv. Matrix sites or sites using a matrix scheme approach.

v. Work-at-home information.

vi. Drop-shipped merchandise.

vii. Any product or service which is not in compliance with all applicable laws and regulations whether federal, state, local or international, including the laws of India.

5. Risk Team checks for Merchant activation

Risk Team–Risk Team will check for the LOB, MCC and other parameters in the merchant sign-up data and will approve/reject the merchant.

Data / information required for Risk check:

- Merchant Business Name – mandatory
- Business Type / Sector - mandatory
- Subsector - mandatory
- Mailing address (Resi & off) (should match with address proof)
- Landmark - mandatory
- Pin Code
- Mobile number - mandatory
- Email id – Sign-up apps validate merchant email id at the time of sign-up.
- Average ticket size (minimum and maximum)
- Business module/brief description of the business\

5.1. Risk scrutiny checks followed before merchant activation

- Business Profile - Product/services category, Owner/director details, Business age, SPOC & Contact information etc.
- An application signed by the merchant.
- Restrict Negative Merchant on boarding - legality of the operation (For e.g. for gambling/Betting and casino Gambling/ Direct Marketing- Subscription /money transfer etc.)
- Financial Checks like 6 months bank statement for high-risk category merchants specially NGO, Trust, Financial services etc.

- Merchant's Business Location Address Capture – The CPV/ Sales person will click photos and mark the longitude and latitude with the help of Maps.
- Merchant CPV Process: An onsite inspection report or verification of business.
- Bank Account validation – Merchant's Bank account details get validated at the time of on boarding by doing penny drop of Rs.1. Sign-up will be treated as Successful only if account validation response received as "Positive"

Merchant can get activated only if merchant meets aforesaid compliance checks.

Once the case is approved from risk, Ops/ Support team activate merchant for transaction. In case merchant is rejected by internal risk, sales team will get communicated about rejection reason and request them not to take forward this particular merchant for on boarding unless exception or queries are not resolved.

5.2. Manage MCC and Merchant Risk Level

5.2.1. Procedures: Quantity of Risk

Conclusion: The quantity of risk is (low, moderate, or high)

Objective: To determine the quantity of risk in merchant processing activities

A Merchant Category Code (MCC) is a four-figure number used to categorize business entities according to the type of products or services the company offers.

To manage and mitigate the risks emerging from newly on boarded merchant it is important to conduct complete due diligence of merchant, including mainly MCC Verification, Ticket size restriction.

MCC Verification – After merchant on boarding MCC helps to ascertain risk level of merchant. Compliance Team ensures accurate MCC code should assign to every merchant, as wrong MCC mapping could cause the highest rates of disputes, also it may impact on wrong rate mapping.

MCC wise rate application – Accurate MCC helps to restrict min. and Max ticket size for that merchant. Also, it helps to define risk level for that merchant.

Risk level assigned to each MCC at the time of on boarding. The risk level considers from several factors including the following:

- Is business conducted online or merchant possess any retail shop for his business?
- Actual line of business (MCC) (business category) under which business is been operated.
- Minimum and maximum ticket size of product.
- Since how long merchant is deals in same line of business, business life cycle.
- Sales volume present and planned.
- Is the percentage of refunds, chargebacks, or fraudulent charges above average?

For example, if you open a corner market in your neighbourhood, the credit card network may tag your account with MCC 5499 as a convenience store. This category is a relatively low-risk category for the merchant provider since your business will likely sell inexpensive items to customers who initiate the transaction and approve the purchases in person.

However, if the merchant deals in money transferring or Non-Financial Institutions – Foreign Currency exchange business, that business comes under MCC 6051. In this case, the code signifies a high-risk category, as the money transfer records a high number of chargebacks and fraudulent charges due to online transfers.

We have specified the risk level of few of categories on the basis of MCC, business LOB and product ticket size: -

MCC	Category	Risk Level
4722	Travel Agencies and Tour Operators	High Risk
4900	Bills and Utilities	Low Risk
5039	Construction materials not elsewhere classified	High Risk

5094	Precious stones and metals, watches and jewelry	High Risk
5137	Men's, women's and children's uniforms and commercial clothing	Low Risk
5139	Commercial footwear	Medium Risk
5399	Miscellaneous General Merchandise	Medium Risk
5411	Groceries and Supermarkets	Medium Risk
5441	Candy, nut and confectionery shops	Medium Risk
1731	Electrical Contractors	Low Risk
5499	Miscellaneous food shops convenience and specialty retail outlets	Medium Risk
5511	Sales, Repair and Services	High Risk
5621	Women's ready-to-wear shops	Medium Risk
5661	Shoe shops	Medium Risk
5691	Apparels and Accessories	Medium Risk
5699	Miscellaneous apparel and accessory shops	Medium Risk
5712	Furniture, home furnishings and equipment shops and manufacturers, except appliances	Very High Risk
6051	Ticket booking, DTH recharge and Money transfer business	High Risk
5732	Electronic Appliances and Mobile	High Risk
5812	Food and Beverages	Medium Risk
5912	Cosmetic	Medium Risk
5940	Bicycle shops sales and service	Low Risk
5947	Gift, card, novelty and souvenir shops	Low Risk
5962	Freelancing Services	High Risk
6012	Payments and Financial Services	High Risk
7298	Health and beauty spas	Very High Risk

7299	Miscellaneous personal services not elsewhere classified	Low Risk
7379	Computer maintenance and repair services not elsewhere classified	Medium Risk
7538	Automotive service shops (non-dealer)	Low Risk
8011	Healthcare	Low Risk
8043	Opticians, optical goods and eyeglasses	Low Risk
8299	Education	Low Risk
8398	Charitable and social service organizations	High Risk

5.2.2. Banned and Prohibited categories restricted from onboarding: -

Please try to avoid pitching the categories mentioned below as those are banned categories and may create challenge in bank approval. List of Negative merchants, which we normally restrict for on-boarding:

MCC	Merchant Category Code
4829	Wire transfers & money orders
5962	Direct Marketing-Travel
5964	Direct Marketing-Catalog Merchant
5966	DM-Outbound telemarketing
5967	DM-Inbound Teleservices
5968	Direct Marketing- Subscription
5969	Direct Marketing-other
5993	Cigar stores and Stands
7273	Dating and Escort
7841	Video tape rental stores
7994	Video games and arcades
7995	Betting and casino Gambling
9754	None-Face-to-Face Gambling

Following is the list of few more prohibited categories which need to be restricted from on-boarding. For reference the complete list has been reproduced below:

- Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services.

  Note: Dating sites and mobile apps are very often fronts for this activity, so ensure not to accept such merchants for on-boarding.

- Alcohol or alcoholic beverages such as beer, liquor, wine, or champagne.

Specifically check grocery or supermarket and obtain an undertaking on merchant letterhead of such merchants stating that they will not sell alcoholic products.

- Bulk marketing tools, which include email lists, software, or other products enabling unsolicited email messages (spam). Merchants/operators might send bulk messages unsolicited, violating this guideline.
- Child pornography which includes pornographic materials involving minors.
- Drugs and drug paraphernalia which include illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms.
- Drug test circumvention aids which include drug cleansing shakes, urine test additives, and related items.
- Endangered species which includes plants, animals or other organisms (including product derivatives) in danger of extinction.
- Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, and related content.
- Government IDs or documents which includes fake IDs, passports, diplomas, and noble titles.
- Offensive goods, crime which includes crime scene photos or items, such as personal belongings, associated with criminals.
- Tobacco and cigarettes which include cigarettes, cigars, chewing tobacco, and related products.
- Traffic devices which include radar detectors/ jammers, license plate covers, traffic signal changers, and related products.

- Weapons which include firearms, ammunition, knives, brass knuckles, gun parts, and other armaments.
- Wholesale currency which includes discounted currencies or currency exchanges.
- Live animals or hides/skins/teeth, nails and other parts etc. of animals.
- Multi-Level Marketing collection fees MLM business are among the most common ones we receive on a regular basis, which could be rejected outright.
- Matrix sites or sites using a matrix scheme approach.
- Work-at-home information.

Post the approvals from underwriting team and Risk team the merchant application is sent to the support and Ops Team. Ops team does the required backend setup based on the feedback and review provided by the risk team and initiates the integration process.

6. Merchant integration

Merchant integration contains details of the integration kit and/or programming language used by the merchant – for example, Java/PHP/.NET, etc. While this is typically informational in nature, it has some relevance in the risk/compliance process especially in the case of mobile app-based integration (Android/iOS). This is explained in more detail in subsequent sections.

6.1. Merchant allowed to send request on Payment Gateway API

Step 1:- Payment Gateway API from which the merchant is allowed to do a POST request to our aggregator's payment request API. Setting in the right API is crucial during Merchant Onboarding. Merchants would be able to direct their users to our payment page only through the pre-registered Payment Gateway API with required Parameters with hash algorithm.

Step 2:- The Payment Gateway validates the request received from the merchant with required parameters.

If all validations are passed, then our hosted page is displayed, else, the Payment Gateway sends appropriate error response to the merchant.

Step 3:- On the Payment Gateway Hosted page, customer selects the payment mode (credit /debit card, Net banking, wallet, UPI) from the payment mode option.

After selecting the payment mode customer fills the required details and Payment Gateway sends request to acquirer for transaction.

Step 4:- After receiving response from acquirer, response is sent to the merchant on merchant's preconfigured return URL only.

If the merchant does not receive a particular response from Payment Gateway, thenhe needs to call our server to server enquiry API to get response.

Enquiry API is shared with the merchant during integration process.

6.2. Merchant whitelisted IPs

List of IP addresses allowed to perform server-server calls (blank means unrestricted access). Please note the crucial difference between URL whitelisting and IP whitelisting. These are NOT the same by any means. URL whitelisting refers to https POST calls which are permitted only from the set of whitelisted URLs as described in previous section. IP whitelisting refers to the IP addresses which are permitted to perform host-to-host or server-to-server calls. These are typically used for API based reconciliation/inquiry, API based refunds, and other similar API calls such as split payment requests.

Using the enquiry API is not mandatory, because of the practical consideration that many merchants use the dashboard UI for all required activity and do not perform API calls.

6.3. Transaction data flows in Hash format

Aggregator server always sends transaction request to Payment Processor with Checksum value, which cannot be easily understood by anyone except authorized parties. Payment processor matches the checksum value using algorithm. VegaaH also ensures that every client and VegaaH should exchange and configure each other's dynamic IP address from which request is going to be received. From dynamic IP address, error URL, response URL client as well as host company, it can be ensured thatrequest is coming from the right source and also helps in avoiding data breaches..

7. System Security Measures

7.1. How Securely Transaction Flow works

1. The customer accesses merchant website and selects checkout option/payment mode option. After this step, the Merchant redirects it to VegaaH Payment Page.
2. Before granting access to VegaaH's payment page, VegaaH authenticates the request raised by the merchant on the basis of Key and IP shared during integration. On the basis of credentials present in the Merchant request, the the aggregator responds with the appropriate error code, in case the Merchant authentication fails. If the merchant is successfully authenticated, a Payment ID is generated by the Payment Gateway. The Payment Gateway response includes the Payment ID and Payment Gateway Card Page URL for redirecting the customer browser from the Aggregator payment page.
3. The Payment Gateway presents the Card Page to the customer to enter the card related sensitive information like Card Number, Card CVV2/CVC2, Card Expiry Date, Card Holder Name etc. The transaction is with status as "IN PROGRESS" on Payment Gateway.
4. VegaaH initiates a Payment Request to the Payment Processor (as per the specified format), comprising Merchant Track Id, and Transaction Amount, Card details, Aggregator Response URL, Aggregator Error URL and other parameters in User Defined Field (UDF).
5. The Payment Processor authenticates VegaaH on the basis of the credentials present in the request. A Payment ID is generated by the Payment Processor on successful validation of the Aggregator. The Payment Processor response includes the Payment ID and the status of the transaction. The Payment Processor responds with the appropriate error code in case the Aggregator authentication fails.
6. The Payment Processor sends the Card Enrolment Verification request to the Card Issuing Bank via the Interchange Directory Server, and on

receiving successful enrolment status customer browser is redirected from Payment Gateway to respective Issuing Bank Access Control Server (ACS).

7. The Issuing Bank ACS presents a Secure Page to enable the Customer enter the 3D Secure Authentication password on the ACS page. Customer provides the 3-D Secure password/ OTP on the ACS page. The ACS authenticates the password/OTP and sends a response back to the Payment Gateway.

8. On successful ACS authentication of the customer, the Payment Processor routes the transaction for Authorization to Acquiring Bank Switch, through the interchange and onto the Issuing Bank Card Host

9. The transaction is authorized by the respective issuing bank host via interchange and the response is sent back to Acquiring Bank Switch and from there back to Payment Processor.

10. . On receipt of response from Payment Processor, VegaaH first validates the IP address from where the response is received. If the response is from Payment Processor IP Addresses, then VegaaH proceeds for further validations, else, declines the transaction.

11. VegaaH receives the Payment ID and status from the Payment Processor. VegaaH now maps the Payment ID, Track ID and Amount with other transaction details in back-end system (database).

12. VegaaH logs the response from the Processor and sends response back to the merchant's Response URL. The transaction status is "Successful/ Failure".

7.2. Benefits of transaction response validation process:

1. VegaaH's system runs inquiry API with acquiring bank to validate payment authorization status.

2. Second leg of security measure happens in real-time.

3. This helps to guard against any losses due to fraudulent activities like tampering of transaction status or of the transaction amount
4. Server--to-server call to retrieve and validate response parameters.
5. Merchant should consider final transaction status before ‘Authorizing’ any sale of goods/services.

8. Transaction monitoring and alerts

Transaction level monitoring segregates in two steps i.e., system level monitoring which happens on real-time basis at the time of transaction initiation and offline monitoring which happens post transaction processing.

8.1. System Level Velocity Checks

Online transaction monitoring which the Payment Gateway system takes care at the time of transaction processing (i.e., on real-time basis).

VegaaH's system has an integrated risk management tool which analyses the risk of each transaction and facilitates the security from suspicious transaction based on complex risk rules in real time. Risk management is a condition-based multilayer rule system, where multiple levels of velocity checks are available.

Velocity checks give the ability to set specific criteria to limit the risk exposure. Velocity filters will reduce the possibility of large volumes of fraudulent transactions. Transactions will be passed through the velocity filter before being processed. If any of these limits are exceeded, transactions will fail with the "fraud velocity" error code.

Typically, the system does a good job of setting up velocity check parameters automatically. Manual intervention is not usually required since the tech team refines the parameters and default velocity requirements on an ongoing basis at the back- end.

Basic velocity Checks have been implemented on various parameters mentioned below:

- Card Number - BIN restrictions
- User and Card Based
- User and IP Based - To know malicious IP Addresses
- Maximum and Minimum Transaction Count for Daily, Weekly, Monthly.
- Limit on Transactions per card
- Time durations available (for access ban): 1 day, 1 week and forever (permanent)
- Refund limits
- Chargeback and Fraud Limits

The above velocities can be set on various currency types.

Rules
Deny when more than 3 transactions per CARDNO in a day.
Deny when more than 5 transactions and 10,000 in value per CARDNO in 1 hour

8.2. Black List Check:

Blacklist controls enable merchants to Block transactions from suspicious Countries, Email IDs, Card numbers or IP addresses.

Deny where Geolocation Country(IPID) = 586(Pakistan)
Deny where Geolocation Country(IPID) = 642(Romania)
Deny where E-mail Domain like DAY.COM
Deny where Card BIN like 468774
Deny where Card BIN like 479947
Deny where Card BIN like 557763
Deny where CARDNO is not found on 'INDIAN_BINS' list(INDIAN_BINS) AND Card BIN is not like 652202 AND Card Issuing Country(VIRTBIN) is not equal to 356(India)

8.3. Rule based checks and red flags

Apart from online risk management tool, VegaaH team also performs post-transaction risk monitoring process.

VegaaH does offline transaction risk monitoring, on the basis of certain velocity checks. VegaaH compliance team has implemented some manual rules and red flags in Payment Gateway, on the basis of which recon system keeps generating exception reports of suspicious transactions.

The Compliance team receives exception reports regularly that enable them to monitor transactional risk.

Following are velocity checks which we have maintained in our payment Gateway, the system filters out suspicious transactions on the basis of these rules..

Suspicious High Value (INR 50,000) Transaction – Very High Risk MCCs
Duplicate Transactions – Same Merchant MID
Duplicate Transactions – International Card on Same Terminal
Card testing scenarios
High CTS Merchant Monitoring - (Chargeback to Sales Ratio - CTS)
High velocity of transaction within specific interval
Unusual activity in connection with the use of Cards or Accounts issued under a particular BIN gift card, prepaid card bin is getting used repeatedly
Merchant Limit Monitoring
Suspicious High Value (INR 1,00,000) Transaction – Very High Risk MCCs
Duplicate Transactions – same card, different IP address
Transactions followed by Fraud-suspect declined transactions with same Card
Transactions followed by Fraud-suspect declined transactions with different Card, but same amount
New Merchant Monitoring – Monitor closely for first 30 days
Different IP Address for same MID and same Card Number
Different MID with same Account Number
Different MID with same IP Address and same Card Number
More than 3 transactions with same Card Number within an Hour
Card Number already marked in Fraud

8.4. Process of suspicious transaction handling

Day 0: Customer initiate transaction from Merchant website.

Day 1: VegaaH Team runs reconciliation process on the basis of aforesaid velocity checks to generate list of suspicious transaction. VegaaH Ops Team analyses each suspicious transaction and conducts risk diligence checks of each and every case.

- **Suspect MID Clearance**
  - Ops allows to segregate suspicious merchant in Cleared and Fraud category. Cases which need to be clear have to be marked as cleared in, so that Pay-out gets generated for those clear set of merchants.
  - For MID, if the status is not clear, they will remain in suspected MID list and pay-out will be not generated for that merchant till the time those are not flagged as “Clear MID”.

Action on final Suspected Merchants: Payment of suspected Merchant will be kept onhold and merchant will be intimated via e-mail as well as phone call about the suspicious transactions. The VegaaH Compliance Team asks for transaction authorization proof from merchant, these documents help us to safeguard ourselves from potential chargebacks which may be expected in future from acquiring banks. Following is the list of documents the Compliance team might require from the merchant merchant to complete risk migration process.

- If the product is in transit or delivered, please share the following Proof of services along with his acknowledgment.
  - Provide the invoice copy against the order idelivered.
  - Proof of services rendered to cardholder along with customer’s acknowledgment
- Customer Manual authorization documents mentioned below.
  - A photo ID of the Credit/Debit Card/Net Banking Account holder who’s Credit/Debit Card/Net Banking Account has been used for this transaction.

- Consent letter is required from customer stating that “Customer has performed this transaction on his own will and he does not have any further dispute with this transaction”
- Any other relevant documents you feel would help validate the customer.

Day 2: Ops team ensures merchant will get intimated about the hold transaction on time. Post receipt of compliance mail, the merchant has to produce all requested documents to validate his transaction. If merchant fails to produce the required documents, a confirmation mail from the merchant stating, “He is unable to produce the document and wants to process refund back to original card holder’s account” is required. Post merchant’s e-mail confirmation Ops team can refund the whole transaction amount to card holder’s account.

If documents provided by merchant are valid or satisfactory to validate suspicious transaction, compliance team can take a call to release the settlement to merchant account.

9. Reconciliation Process

9.1. What is Reconciliation?

Reconciliation is the process of matching transactions that have been recorded internally against daily statements from external sources such as banks to see if there are differences in the records.

The objective of doing reconciliations is to ensure that the internal System Statement agrees with the bank statement. Once any differences have been identified and rectified, both internal and external records should be equal in order to demonstrate good financial health.

Reconciliation is performed on a regular and continuous basis on all balance sheet accounts as a way of ensuring the integrity of financial records. This helps uncover omissions, duplication, theft, and fraudulent transactions

The reconciliation process is usually automated, using VegaaH System. However, since some transactions may not be captured in the system, manual involvement is required to identify such unexplained differences

The first step is to compare transactions in the internal System and the bank account to see if the payment and deposit transactions match in both records. Identify any transactions in the bank statement that are not backed up by any evidence.

Sometimes, errors may occur in the bank statement, thus, producing some differences between the internal System Statement and bank statement. Possible errors include duplication errors, omissions, transposition, and incorrect recording of transactions.

The errors should be added, subtracted, or modified on the bank statement to reflect the right amount. Once the errors have been identified, the bank should be notified to correct the error on their end and generate an adjusted bank statement.

Below are the scenarios for recon

- VegaaH and Payment Processor file Match
    - In this scenario only recon file will generated.

- VegaaH and Payment Processor file mismatch less records in VegaaH File

  - In this scenario 2 files are generated: recon and unrecon.
  - Ops team needs to check Unrecon file and investigate the reason of Unrecon transaction
  - If record exists at the payment provider end, VegaaH initiates payment processor enquiry API and updates the un recon transaction status
  - Perform the recon process again.

- VegaaH and Payment Processor file mismatch less records in Payment Processor file

  - The Payment Processor should be notified to correct the error on their end and generate an adjusted statement and share with VegaaH
  - Perform the recon process again

On completion of the recon process VegaaH ops team proceeds with the merchant settlement.

10. CHARGEBACK MANAGEMENT:

10.1. What is a chargeback?

A Chargeback is a process that allows debit and credit card holders to reverse transactions when there is a problem with the goods or services, they have purchased using their cards.

Chargeback or retrieval request is generally received from the respective Acquiring bank which processes online PG transactions on behalf of request from VegaaH

10.2. Handling 1st Level of Chargeback cases:

VegaaH receives chargeback intimation mail from the acquirer, all requested documents are to be submitted via mail.

The step-by-step process of chargeback is explained below:

1. Acquirer receives chargeback notification from their acquiring banks.
2. Acquirer notifies VegaaH through email by providing disputed transaction details and documents required from merchants to remedy the chargeback. The merchant needs to respond within 5 days of receiving the chargeback notification.
3. VegaaH is expected to provide their chargeback response over e-mail within target date.
4. After submitting the documents, Acquiring Bank verifies the details sent by VegaaH.
5. If VegaaH does not respond within the stipulated timeline, the acquiring bank will close the case in favour of the customer.

Chargeback information is received in the following format-

1. VegaaH transaction ID.
2. Transaction Date.

3. Transaction/chargeback Amount.
4. Reason of chargeback.
5. Target date to provide reply. – Deadline for submitting actual documents from merchant to Bank.

10.3. Chargeback resolution process

As mentioned in aforesaid notes, VegaaH receives chargeback intimation from Acquiring Bank. As soon as VegaaH receives the chargeback, further payments of that merchant are put on hold. This amount can be released to merchant only if acquiring bank closes the case in favour of Merchant.

1. On the basis of intimation received, the VegaaH Compliance Team sends out e-mail to merchant's authorised email id and asks for the following set of documents (depending on chargeback reason) from merchant.
    a. Legible copy of Online authorization details
    b. Order details
    c. Proof of services rendered (invoice copy) to cardholder along with his acknowledgment
    d. E-mail confirmation from customer for withdrawal of dispute along with his photo id proof
    e. Any other documentation that may assist in verifying the authenticity of these transactions.
2. VegaaH Team needs to ensure that Chargeback Target Date is clearly communicated to the Merchant.
3. Merchant needs to share the documents within mentioned target date, so that VegaaH can assist merchant to resolve disputed case in Merchant's favour.
4. VegaaH Operation's team verify the document and sends it to the acquirer for further verification.

5. Acquiring bank is ultimately responsible for determining the resolution of chargebacks. If case gets resolved in customer's favour, customer's account get credited from his issuer bank. If chargeback resolves in merchant's favour, hold amount gets released and will be settled in merchant's favour.

An E-mail goes to merchant communicating about the disputed transaction and request for producing requested document to defend chargeback case.

10.4. Handling Pre-Arbitration and 2nd Chargeback cases

Once the issuing bank reviews the submission made by the merchant, they can close the case in favour of the merchant or decline the merchant claim and re-initiate a 2nd level dispute (Pre-Arbitration, 2nd chargeback).

In case of a Pre-Arbitration/ 2nd Chargeback, acquirer will notify the same to VegaaH along with the required documentation (Acquiring bank may request additional documentation apart from the one already submitted at the time of 1st chargeback).

Acquiring bank will review the documentation and determine if the case is strong enough to defend. Acquiring bank may refuse to defend the case in this stage and the case will be closed against the merchant.

10.5. Chargeback Timeframe / chargeback Cycle

Please be advised that any transaction can be disputed within the 120 days from the date the transaction posted to his account, however for couple of chargeback reason it can be extended up to 180 days.

Merchant should retain the transaction related details (proof of delivery/invoice etc.) for each transaction for minimum 6 months.

CHARGEBACK	
Chargeback types	**Timeframe**
1st Level Chargeback	1 Day to 5 Day **(Calendar Days)**
2nd Level Chargeback & Pre-arbitration	1 Day to 3 Day **(Calendar Days)**

10.6. Types of Disputes

Disputes can be

- Customer initiated (Normal Chargebacks)
- Bank Initiated (Technical Chargebacks)

10.6.1. Examples of Customer initiated Disputes

- Transaction not authorised/Fraud
- Goods/Services not received or not as Described
- Cancelled transaction but credit not received
- Transaction Not Recognised
- Duplicate Billing

10.6.2. Examples of Bank Initiated Disputes

- Late settlement by Merchants
- Authorisation/Invalid authorisation obtained by ME
- Retrieval Request Not Fulfilled

10.7. Why do Disputes arise and what all documents are required from the merchant for dispute reason?

- Non-Receipt of Item/Service- In this case, the customer claims that they never received the product(s) or the service they purchased. Document required – A signed proof of delivery from a shipping company showing that the item has been received by the customer. For services, any documented proof/email which proves that the customer has received the service.
- Duplicate Payment – This chargeback reason code is used when the customer claims that he has been charged more than once for the same product/service. Document required – Any documented proof suggesting that you have provided the service for each of the transactionor provide signed proof of delivery for each of the orders.
- Incorrect Amount – This is when the customer claims that he/she was charged more than they were agreed to. Document required – an itemized invoice showing the charged amount is correct. Along with a screen-shot from the product page of your website showing the amount which has been charged.

- Paid by other means- This is when the customer claims that he/she already paid you for the same service/item through any other means. (Example- a different credit card, debit card, Net Banking, cash). Document required – any documented proof suggesting that the other payments were for different order and item/service was provided to the customer.
- Defective/Damaged item – If the item was defective / damaged upon receipt. Document required- provide documented proof explaining why a refund is not due. Proof of disclosure of the return/refund policy along with the proof what was ordered.
- Credit not Processed/Cancelled Transaction – This reason code is used when the customer has either cancelled the transaction, or a promised credit was not issued.

Unauthorized Transaction – In case a transaction been disputed as unauthorized (fraud), the merchant must provide all the required documents, (signed proof of delivery, invoice, order confirmation email etc.).