मध्य प्रदेश ग्रामीण बैंक

Madhya Pradesh Gramin Bank

Payment Aggregator

&

Payment Gateway

Onboarding Policy

IT DEPARTMENT

(Formulated on 25-10-2023)

Table of Contents

Payment Aggregator & Payment Gateway Onboarding Policy

Payment Aggregator & Payment Gateway Onboarding Policy

1. Objective

1.1. This policy document outlines the guiding principles in respect of various aspects relating to onboarding of Payment Aggregators.

1.2. The policy shall be governed by Payment & Settlement systems act 2007,RBI/ Government and Bank's guidelines/circulars

1.3. The Policy aims at fostering a culture of compliance, innovation, quick adoption of technology for undertaking Payment Aggregator Business for qualitative improvement in customer service, business and profitability and increasing digital transactions.

2. Definitions

2.1. Payment Aggregators are service providers through which e-commerce merchants can process their payment transactions. Aggregators allow merchants to accept various payment instruments and bank transfers without having to set up a merchant account with a bank or card association. The payment aggregator is facilitating the collection of payment from the consumer via credit cards, debit card or bank transfer to the merchant. The merchant is paid by the aggregator in 1-3 working days. These services are the most popular forms of payment.

2.2. A Payment Gateway is an e-commerce software application, software that allows online transactions to take place. It is a pass-through mechanism through which cards, net banking and e-wallet payments are done. Payment gateways offer a means to accept online payments.

2.3. Both payment gateways and payment aggregators are inclusive. A payment aggregator need not act as a payment gateway, but a payment gateway will need an aggregator. A payment aggregator can offer a payment gateway but a payment gateway cannot offer a payment aggregator.

Payment Gateways play the role of an intermediary with merchants and customers who want to pay for any goods or services they are purchasing from the site. A payment aggregator is more an interface through which said intermediaries accept payments and make settlements.

3. Outsourcing of Technology for Payment Aggregator

3.1. Outsourcing is successful as it increases product quality, lowers costs substantially, or both. Outsourcing leads to the ability to utilize the technological know-how of other organizations. This allows businesses to find the specific requirements they need to implement their target objectives Outsourcing leads to adoption of economical approach for developing/improvising products and services.

3.2. Payment Aggregator business is highly technology driven and requires quick roll out of products and services and quick adoption of security and other measures mandated by PCIDSS [Payment Card Industry Data Security Standards] requirements. This activity shall preferably be done in-house. In case this has to be outsourced, Bank shall ensure adherence to Outsourcing Policy.

3.3. The Reserve Bank of India has issued guidelines on Outsourcing to provide guidance to banks, to adopt sound and responsive risk management practices for effective oversight, due diligence and management of risk arising from outsourcing activities.

3.4. RBI's instructions contained in its circulars issued vide the following would be applicable.

a) DBOD.NO.BP 40/21.04.158/2014-15 dated 3rd November 2006
b) DBOD.NO, BP 64/21.04. 158/2007-08 dated 3rd March 2008
c) DBOD.NO.BP,97/21.04.158/2008-09 date 11th December 2008
d) DBS.CO.PPD.BC.5/11.01.005/2008-09 dated 22nd April 2009
e) DBR.NO.BP,BC.76/21.04.158/2014-15 dated 11th March 2015

The guidelines are applicable to outsourcing arrangements entered into by a bank with a service provider located in India or elsewhere.

3.5. As per Bank's Outsourcing Policy, it is necessary to exercise control at strategic points by devising an appropriate supervisory mechanism over the outsourced activities.

3.6. While considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational, reputational factors. The bank should consider whether the service providers systems are compatible with its own and also whether their standards of performance, including in the area of customer service, are acceptable to it where possible, the bank should obtain independent reviews and market feedback on the service provider to supplement its own findings.

3.7. The failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements by either the service provider or the outsourcing bank can lead to financial losses /reputational risk for the bank and could also lead to systemic risks within the entire banking system in the country. It would therefore be imperative while outsourcing the activities to ensure effective management of these risks.

3.8. Access to various data would be required to restricted to areas required to perform outsourced functions only and in no case details of the customer and other sensitive data to be shared with the agents so as to impair confidentiality

3.9. Legal Obligations. Regulatory and supervisory requirements :

a) It will be obligatory on the part of service provider/outsourcing agent to inform change in management and the key persons monitoring the arrangements to ensure continuity of operations.

b) Due diligence in relation to outsourcing, to consider all relevant laws, regulations, guidelines and conditions of approval, licensing or registration should be done.

c) Outsourcing arrangements should not affect the nights of a customer against the bank, including the ability of the customer to obtain redressal as applicable under relevant laws.

d) Outsourcing, whether the service provider is located in India or abroad should not impede or interfere with the ability of the bank to effectively oversee and manage its activities or impede the Reserve Bank of India in carrying out its Supervisory functions and objectives.

e) A robust grievance redressal mechanism should be available, which in no way should be compromised on account of outsourcing.

f) The service provider, if it is not a subsidiary of the bank, should not be owned or controlled by any director or officer/employee of the bank or their relatives having the same meaning as assigned under sub section (77) of Section 2 of the Companies Act, 2013.

3.10. The bank should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

3.11. The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by a competent authority on their legal effect and enforceability. Every such agreement should address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. The agreement should be sufficiently flexible to allow the bank to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations.

4. Authorisation from RBI

4.1. Banks provide PA services as part of their normal banking business and therefore do not require a separate authorization from RBI Non-Bank PAS must have authorization from RBI under the Payment and Settlement Systems Act, 2007 (PSSA).

4.2. PGs shall be considered as technology providers' or outsourcing partners' of banks, as the case may be. In case of a bank PG, the guidelines issued by Reserve Bank of India, Department of Regulation (DoR) vide circular No.DBOD.NO.BP 40/21.04.158/2006-07 dated November 3, 2006 on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks" and other follow up circular(s) shall be applicable.

5. Services Covered

5.1. The Payment Aggregator must offer payment options through credit card debit card, bank account, wallet, Unified Payments Interface (UPI), etc Payment Gateways and Payment Aggregators may also provide services which include generation of settlement via netting of the funds received by the merchants on boarded by them.

5.2. The entities may also provide cross border settlement services subject to compliance of guidelines issued by Foreign Exchange Department (FED RBI) on Online Payment Gateway Service Providers (OPGSPs). (Please refer to Para 6)

5.3. Payment Aggregators shall provide the Merchants (i) online transaction processing across various banks 002Fcard gateways to enable the merchant's customers to conduct online transactions, (ii) recurring transaction processing on bank accounts /cards accounts (through NACH, banks, card networks etc.. (iii) Reconciliation, MIS, transaction-to-fund flow match, etc., (IV) Transaction support, technology interface support, etc.

5.4. Payment Aggregator shall provide the bank one standardized - centralized manner of dealing with the bill-data of various utilities.to take care of MIS, reconciliation, consolidated pay outs and other service delivery aspects, etc..

5.5. Cross border transactions as per Para 6

6. Requirements for Operationalization of Cross Border Transaction

6.1.1. This Facility shall be provided through AD Category branches.

6.1.2. The outsourcing related to overseas operations of Indian banks would be governed by both, these guidelines and the host country guidelines Where there are differences, the more stringent of the two would prevail However where there is any conflict, the host country guidelines would prevail.

6.1.3. Details of each such arrangement, as and when entered into, shall be reported by the bank to the Foreign Exchange Department, Central Office, Reserve Bank of India, Mumbai.

6.1.4. For operationalizing such arrangements. banks shall :

i. Carry out the due diligence of the OPGSP
ii. Maintain separate Export and Import Collection accounts in India for each OPGSP,
iii. Domestic entities functioning as intermediaries for electronic payment transactions and intending to undertake cross border transactions shall maintain separate accounts for domestic and cross border transactions.
iv. Satisfy as to the bonafides of the transactions and ensure that the related purpose codes reported to the Reserve Bank are appropriate;
v. Submit all the relevant information relating to any transaction under such arrangements to the Reserve Bank, as and when advised to do so; and
vi. Conduct the reconciliation and audit of the collection accounts on a quarterly basis

6.1.5. Processing of export related receipts through Online Payment Gateway Service Providers (OPGSPs)

AD Category-I branches may offer the facility of repatriation of export related remittances by entering into standing arrangements with OPGSPs subject to the following conditions.

a) This facility shall only be available for export of goods and services of value not exceeding the limit fixed by RBl (presently USD 10,000 or equivalent per transaction).

b) Resolution of all payment related complaints of exporters in India shall remain the responsibility of the OPGSP concerned.

c) Start-up can realize the receivables of its overseas subsidiary and repatriate them through Online Payment Gateway Service Providers (OPGSPs).

6.1.6. Import related payments through Online Payment Gateway Service Providers (OPGSPs).

AD Category-I branches may offer facility of payment for imports of goods and software by entering into standing arrangements with the OPGSPs subject to the following

a) This facility shall only be available for import of goods and services of value not exceeding the limit fixed by RBI (presently US0 2,000 or equivalent per transaction).

b) The AD Category branch will obtain a copy of invoice and airway bill from the OPGSP containing the name and address of the beneficiary as evidence of import and report the transaction in R- Return under the foreign currency payment head.

7. Eligibility

7.1. Entities undertaking Payment Aggregation and Payment Gateway activity shall be a company incorporated in India under the Companies Act, 1956/ 2013.

7.2. Payment Gateways and Payment Aggregators shall deal with only those merchants who have a physical presence in the country.

7.3. The Memorandum of Association (MoA) of the entity must cover the activity of operating as a Payment Gateway and Payment Aggregator.

7.4. Capital Requirements -

7.4.1. Existing PAs • Networth of Rs.15 Crore by 31-03-2021, & Rs. 25 Crore by 31-03-2023. Rs. 25 Crore to be maintained at all times.

7.4.2. New PAs Minimum Rs.15 Crore initially; Rs.25 Crore in end of third FY; Rs. 25 Crore at all times there after.

7.4.3. Approval of deviation related to Networth would be under the delegation of Chairman.

(Net-worth shall consist of paid up equity capital, preference shares which are compulsorily convertible into equity capital, free reserves. balance in share premium account and capital reserves representing surplus arising out of sale proceeds of assets but not reserves created by revaluation of assets adjusted for accumulated loss balance, book value of intangible assets and deferred revenue expenditure, if any. Compulsorily convertible preference shares can be either non-cumulative or cumulative, and they should be compulsorily convertible into equity shares and the shareholder agreements should specifically prohibit any withdrawal of this preference capital at any time. Entities having Foreign Direct Investment (FDI)/Foreign Portfolio Investment (FPI) I Foreign Institutional Investment (FI) shall also meet the capital requirements as applicable under the extant Consolidated FDI policy guidelines of Government of India and foreign exchange management regulations on this subject).

7.5. Governance-

7.5.1. The entity shall be professionally managed. The promoters of the company shall satisfy the fit and proper criteria prescribed by RBI.

7.5.2. PAs shall disclose comprehensive information regarding merchant policies, customer grievances, privacy policy and other terms and conditions on the website and / or their mobile application.

7.5.3. PAs shall have a Board approved policy for disposal of complaints / dispute resolution mechanism/ time-lines for processing refunds, etc., in such a manner that the RBI instructions on Turn Around Time (TAT) for resolution of failed transactions issued vide DPSS COPD No 629/02.01.014/2019-20 dated September 20, 2019 are adequately taken care of Any future instructions in this regard shall also be adhered to by PAs.

7.5.4. PAs shall appoint a Nodal Officer responsible for regulatory and customer grievance handling functions. PAs shall prominently display details of the nodal officer on their website.

7.5.5. PAs shall appoint a Relationship Manager for Bank.

8. Due Diligence

8.1. Proper due diligence at the bank level shall be done while processing the onboarding request of entity.

8.2. The Payment Gateway I Aggregator should be well established in the business and should be in business for a reasonable period - at least twelve months. In case of new accounts, whether canvassed or not, enhanced due diligence shall be done before deviation is approved.

8.3. There should be no adverse market reports

8.4. If entity is already enrolled by another institution, status report from the institution/banker shall be obtained.

8.5. CIBIL/CRILC/ Credit Bureau report for the business entity and its partners/ directors/promoters/proprietors/authorized signatories shall be generated and should be acceptable to the Bank. Credit Information Report should not contain any overdue or legal action for recovery of dues / written-off accounts If the issues are technical or the details are not updated, based on available documentary evidence, the competent authority may relax the condition by incorporating full details in the proposal.

8.6. The documents (like financial statements, license copies etc) submitted by the entity should be scrutinized with the same degree of prudence as that for a credit proposal.

8.7. Inspection of Business Location shall be done by authorised Bank official/s and the findings should be satisfactory.

9. Empanelment/depanelment and Review of Operations

9.1. Selection of PA/PG shall be on the basis of transparent process, which must evaluate the partnership on various parameters including technical, financial and other parameters.

9.2. Bank may have avail service of limited number of PAs and PGs, not exceeding 10 PAs and 5 PGs.

9.3. Review of Service providers of PAs/PGS shall be done at least every 3 years.

9.4. PAs an PGs empanelment and depanelment will be done by the General Manager.

9.5. Bank may depanel PA/PG service contract at any of following reasons;

a) Activity level of service provider is low or unsatisfactory.
b) Customer complaints are not addressed effectively.
c) IT system/ interface/ Information Security does not comply with Bank's requirements.
d) Charges not applied /shared as agreed with bank.
e) The firm loses license/authorisation to continue with concerned business.

9.6. Review of Operations and profitability shall be undertaken on an annual basis for existing on-boarded aggregator.

10. Merchant Onboarding Pre-requisites

10.1. Bank shall not onboard Payment Gateway and Aggregators, who are onboarding Merchants (a) dealing in prohibited products and services attached as Annexurel and (b) avoidable Merchant Categories as per Annexure-l (These annexures are same as per Merchant Acquisition Business of Card Product Department).

10.2. PAs shall have a Board approved policy for merchant on-boarding.

10.3. The Payment Gateways and Payment Aggregators shall ensure compliance to KYC/AML requirements while onboarding merchants.

10.4. The Payment Aggregators shall undertake background and antecedent check of the merchants, to ensure that such merchants do not have any malafide intention of duping customers.

10.5. The merchant's website shall clearly indicate the terms and conditions of the service, time-line for processing returns/refunds and compensation payable, compliant with RBI guidelines of harmonization of TAT.

10.6. The PA shall be responsible to check PCI-DSS (Payment Card Industry-Data Security Standard) and PA-DSS (Payment Application Data Security Standard) compliance of infrastructure of merchant onboarded.

10.7. Merchant site should not save customer data.

10.8. The agreement with merchant shall have provision for security / privacy of customer data PAs agreement with merchants shall include compliance to PA .DSS and incident reporting obligations. The entity shall obtain periodic security assessment reports either based on the risk assessment (large Or small merchants) and / or at the time of renewal of contracts.

10.9. The Payment Gateways and Payment Aggregators shall provide all collaterals, demo, integration test kits to understand the various features of the services being offered.

11. Safeguards against Money Laundering (KYC/AML/CFT)

11.1. The Know Your Customer (KYC)/Anti-Money Laundering (AML)/ Combating Financing of Terrorism (CFT) guidelines issued by the Department of Banking Regulation (DBR), RBI, in their "Master Direction -- Know Your Customer (KYC) Directions"updated from time to time, shall be complied with by all the Payment Aggregators & Payment Gateways.

11.2. Payment Aggregators and Payment Gateways shall also comply with the provisions of Prevention of Money Laundering Act, 2002 and Rules framed thereunder, as amended from time to time.

12. Customer Grievance Redressal and Dispute Management Framework

12.1. Payment Aggregators should put in place a formal, publically disclosed customer grievance redressal and dispute management framework, including designating a nodal officer to handle the customer complaints / grievances and the escalation matrix.

12.2. Payment Aggregators should appoint a Nodal Officer responsible for regulatory and customer grievance handling functions. Details of the Nodal Officer for customer grievance should be prominently displayed on their website.

12.3. Payment Aggregators should have a dispute resolution mechanism binding on all the participants which shall contain transaction life cycle, detailed explanation of types of disputes, process of dealing with merchants compliance, responsibilities of the parties, documentation, reason codes, procedure for addressing the grievance, processing of refunds, compensation for failed transactions, turnaround-time for each stage etc..

13. Operation of Account for Settlement of Transactions

A. Domestic Transactions

13.1. PAs shall maintain the amount collected by them in an escrow account with any scheduled commercial bank.

13.2. Escrow account balance shall be maintained with only one scheduled commercial bank at any point of time. In case there is a need to shift the escrow account from one bank to another, the same shall be effected in a time-bound manner without impacting the payment cycle to the merchants under advice to RBI and Bank.

13.3. In the processing of an online transaction the following timelines are involved :

- 'To' - date of charge / debit to the customer's account against the purchase of goods / services.
- Ts' - date of intimation by the merchant to the intermediary about shipment of goods.
- 'Td' - date of confirmation by the merchant to the intermediary about delivery of goods to the customer.
- 'Tr'- date of expiry of refund period as fixed by the merchant.

13.4. Amounts deducted from the customer's account shall be remitted to the escrow account maintaining bank on Tp+0/ Tp+1 basis. The same rules shall apply where wallets are used as a payment instrument.

13.5. Final settlement with the merchant by the PA shall be effected as under:

13.5.1 Where PA is responsible for delivery of goods / services the payment to the merchant shall be not later than on Ts + 1 basis.

13.5.2 Where merchant is responsible for delivery, the payment to the merchant shall be not later than on Td + 1 basis.

13.5.3 Where the agreement with the merchant provides for keeping the amount by the PA till expiry of refund period, the payment to the merchant shall be not later than on Tr + 1 basis.

13.6. Credits towards reversed transactions (where funds are received by PA) and refund transactions shall be routed back through the escrow account unless as per contract the refund is directly managed by the merchant and the customer has been made aware of the same.

13.7. At the end of the day, the amount in escrow account shall not be less than the amount already collected from customer as per 'T' or the amount due to the merchant.

13.8. PAs shall be permitted to pre-fund the escrow account with own / merchant's funds. However, in the latter scenario, merchant's beneficial interest shall be created on the pre-funded portion.

13.9. The escrow account shall not be operated for 'Cash-on-Delivery transactions.

13.10. Permitted credits / debits to the escrow account shall be as set out below :

13.10.1. **Credits**

a) Payment from various customers towards purchase of goods/services.
b) Pre-funding by merchants/PAS
c) Transfer representing refunds for failed/disputed/returned/cancelled transactions.
d) Payment received for onward transfer to merchants under promotional activities, incentives. cash-backs etc

13.10.2. **Debits**

a) Payment to various merchants / service providers.
b) Payment to any other account on specific directions from the merchant.
c) Transfer representing refunds for failed / disputed transactions.
d) Payment of commission to the intermediaries. This amount shall be at pre-determined rates / frequency.
e) Payment of amount received under promotional activities incentives. cash-backs, etc

13.11. For banks the outstanding balance in the escrow account shall be part of the net demand and time liabilities' (NDTL) for the purpose of maintenance of reserve requirements. This position shall be computed on the basis of the balances appearing in the books of the bank as on the date of reporting

13.12. The entity and the escrow account banker shall be responsible for compliance with RBI instructions issued from time to time.

13.13. Settlement of funds with merchants shall not be co-mingled with other business, if any, handled by the PA.

13.14. PAs shall submit the list of merchants acquired by them to the bank, where they are maintaining the escrow account and update the same from time to time. The bank shall ensure that payments are made only to eligible merchants / purposes. There shall be an exclusive clause in the agreement signed between the PA and the bank maintaining escrow account towards usage of balance in escrow account only for the purposes mentioned above.

13.15. No interest shall be payable by the bank on balances maintained in the escrow account, except when the PA enters into an agreement with the bank maintaining the escrow account, to transfer "core portion" of the amount, in the escrow account, to a separate account on which interest is payable, subject to the following.

13.15.1 The bank shall satisfy itself that the amount deposited represents the "core portion" after due verification of necessary documents

13.15.2 The amount shall be linked to the escrow account, i.e. the amounts held in the interest-bearing account shall be available to the bank, to meet payment requirements of the entity, in case of any shortfall in the escrow account.

13.15.3 This facility shall be permissible to entities who have been in business for 26 fortnights and whose accounts have been duly audited for the full accounting year. For this purpose, the period of 26 fortnights shall be calculated from the actual business operation in the account.

13.15.4 No loan is permissible against such deposits. Banks shall not issue any deposit receipts or mark any lien on the amount held in such form of deposits.

13.15.5 Core portion shall remain linked to the escrow account The escrow account balance and core portion maintained shall be clearly disclosed in the auditors' certificates submitted to RBI on quarterly and annual basis.

B. Cross Border Transactions

I. Exports of Goods and Services

13.16. Opening and Maintenance of Account

13.16.1 AD Category branches providing such facilities shall open a NOSTRO collection account for receipt of the export related payments facilitated through such arrangements. Where the exporters availing of this facility are required to open notional accounts with the OPGSP, it shall

be ensured that no funds are allowed to be retained in such accounts and all receipts should be automatically swept and pooled into the NOSTRO collection account opened by the AD Category branches

13.16.2 A separate NOSTRO collection account may be maintained for each OPGSP or Bank should be able to delineate the transactions in the NOSTRO account of each OPGSP.

13.17. The following operations shall be permitted in the account

13.17.1 Credits

i. The only credit permitted in the same OPGSP Export Collection account will be repatriation from the NOSTRO collection accounts electronically.

13.17.2 Debits

ii. Repatriation of funds representing export proceeds to India for credit to the exporters' account

iii. Payment of fee/commission to the OPGSP as per the predetermined rates / frequency/ arrangement to the current account of the OPGSP, and

iv. Charge back to the importer where the exporter has failed in discharging his obligations under the sale contract.

13.18. The balances held in the NOSTRO collection account shall be repatriated and credited to the respective exporter's account with a bank in India immediately on receipt of the confirmation from the importer and, in no case, later than seven days from the date of credit to the NOSTRO collection account.

II. Import of Goods and Services

13.19. The balances held in the Import Collection account shall be remitted to the respective overseas exporter's account immediately on receipt of funds from the importer and, in no case, later than two days from the date of credit to the collection account.

13.20. A separate account may be maintained for each OPGSP or Bank should be able to delineate the transactions in the account of each OPGS.

13.21. The following operations shall be permitted in the account.

13.21.1 Credits

i. Collection from Indian importers for online purchases from overseas exporters electronically through credit card, debit card and net banking and ;
ii. Charge back from the overseas exporters.

13.21.2 Debits

i. Payment to overseas exporters in permitted foreign currency,
ii. Payment to Indian importers for returns and refunds
iii. Payment of commission at rates/frequencies as defined under the contract to the current account of the OPGSP, and
iv. Bank charges

14. Transaction Limits

14.1 Subject to exceptions mentioned at para 14.2 Limits on transaction amounts for a particular payment mode shall not be placed by Payment Gateways and Payment Aggregators. The responsibility for placing such transaction amount limit shall lie with the issuing bank or issuing entity; for instance, the card issuing bank shall be responsible for placing limits on cards issued by them based on the customer's credit worthiness, spending nature, profile, etc

14.2 Exceptions (Para 6)

i. Cross border settlement, both inward and outward, shall be subject to limits prescribed by RBI, Foreign Exchange Department relating to Online Payment Gateway Service Providers (OPGSPs)

15. Security, Fraud Prevention and Risk Management Framework

15.1 The Payment Gateways and Payment Aggregators shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds**.**

15.2 The Payment Gateways and Payment Aggregators shall put in place Board approved Information Security policy for the safety and security of the payment systems operated by them, and implement security measures in accordance with this policy to mitigate identified risks. Indicative IT security recommendations are provided in Annexure Ill for adoption by the Payment Aggregator and Payment Gateways.

15.3 The Payment Gateways and Payment Aggregators shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and breaches.

Any incident or breach shall be reported to the Bank and other relevant agencies/authorities.

15.4 The Payment Gateways and Payment Aggregators shall not store the customer card credentials within their database or the servers accessed by the merchants.

15.5 All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required

15.6 The Payment Gateways and Payment Aggregators shall submit the System Audit Report, including cyber security audit conducted by CERT-In empanelled auditors, within two months of the close of their financial year to the Bank.

15.7 The Payment Gateways and Payment Aggregators shall not invoke ATM PIN as a factor of authentication for card transactions.

15.8 The entities shall ensure compliance of guidelines on additional factor of authentication (AFA) & receiving transactions issued by RBI.

15.9 The entities shall obtain appropriate Cyber Security / Applicable Insurance Policy to guard against risk of unauthorized transactions.

15.10 All refunds shall be made to original method of payment unless specifically agreed by the customer to credit an alternative mode

16. Schedule of Charges

16.1 Schedule of Charges shall be mutually decided between the Bank and the entities. No additional Charges shall be levied by the entities on the Merchants.

16.2 The maximum charge shall be within the limits fixed by RB/ Government.

17. Roles and Responsibilities of Bank and Other Stakeholders

17.1 The agreements between Payment Gateways and Payment Aggregators merchants, acquiring banks, and all other stake holders shall clearly delineate the role and responsibilities in sorting/handling complaints, refund/failed transactions, return policy, customer grievance redressal (including turnaround time for resolving queries), dispute resolution mechanism, reconciliation, etc.

17.2 The Payment Gateways and Payment Aggregators shall ensure that neither the merchants on-boarded by them pass on MDR (Merchant Discount Rate) charges to customers while accepting payments through debit cards nor will they separately charge customers in lieu of MDR on debit cards Information on other

charges such as convenience fee, etc., if any, being levied shall be displayed by the Payment Gateways and Payment Aggregators before the payment is made by the customer.

18. Defined Operational Guidelines

18.1 Standard Operating Procedure, consistent with this policy, shall be put In place.

19. Delegation

19.1 Operational Process Documents, based on this Policy, shall be cleared by CORM for implementation.

19.2 On-boarding of PA/PG as per Policy shall be approved by GM in charge of Transaction Banking Department.

19.3 On-boarding of PA/PG with deviation shall be approved by Executive Director and above.

19.4 All operation aspects shall be approved by GM in charge of Transaction Banking Department**.**

20. Review of Business and Updation of Policy

20.1 Review of Business covered under this Policy shall be done at least once in a year by Board.

20.2 This Policy shall be in force till next review

Reference

Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries – DPSS.CO PD No.1102 102.14.08/ 2009-10 dated 24.11-2009

Processing and settlement of import and export related payments facilitated by Online Payment Gateway Service Providers - RBI/2015-16/185 dated 24.-09-2015

Master Direction - Export of Goods and Services - RBL/FED/2015-16/11 FED Master Direction No. 16/2015-16 dated 01-01-2016 (updated as on 01-04-2019)

Master Direction - Import of Goods and Services - RBI/FED/2016-17/12 FED Master Direction No. 17/2016-17 dated 01-01-2016 (updated as on 01-04-2019)

Guidelines on Regulation of Payment Aggregators and Payment Gateways - RBI/DPSS/2019-20/174 dated 17-03-2020

Annex-I : Indicative list of prohibited products, services and transactions (This list is indicative and not exhaustive. All merchants must ensure total compliance with other prohibited goods/services as per laws of India)

(Common List for Merchant Business Acquisition & Payment Aggregator On-boarding)

Part – I : Prohibited or restricted Goods/Services

1. Fire arms, Hazardous materials

Firearms or Explosives or pyrotechnic devices or supplies, Weapons including firearms, ammunition, knives, brass knuckles, gun parts, Hazardous materials which includes combustibles, corrosives, fireworks and related goods; Toxic, flammable, and radioactive materials and substances.

2. Fake/banned/illegal Goods and services

Fake products or autographs ; counterfeit stamps ; Government IDs Or documents which includes fake IDs, passports, diplomas, and noble titles llegal goods which includes materials, products, or information promoting llegal goods or enabling illegal acts.

3. Regulated goods for which authorization is not obtained

Tobacco and cigarettes which includes cigarettes, cigars, chewing tobacco, and related products; Alcohol which includes Alcohol or alcoholic beverages such as beer, liquor, wine, or champagne 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

4. Fake/banned Drugs and unlicensed Medical Practitioner, Illegal tests

Banned / illegal drugs or other controlled substances or drug accessories and Miracle cures which include unsubstantiated cures, remedies or other items marketed as quick health fixes; 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 Drug test circumvention aids which includes drug cleansing shakes, urine test additives, and related items.

5. Trading of Live/endangered Animals/species, body parts

Live animals or hides/skins/teeth, nails and other parts etc. of animals endangered species, which includes plants, animals or other organisms (including product derivatives) in danger of extinction Body parts which includes organs or other body parts.

6. Activities involving copyright violation

Copyrighted media which includes unauthorised copies of books, music, movies, and other licensed or protected materials; Copyrighted software which includes unauthorised copies of software, video games and other licensed or protected materials, including OEM or bundled software Copyright unlocking devices designed to circumvent copyright protection; Cable descramblers and black boxes which includes devices intended to obtain cable and satellite signals

7. Adult goods and services

Adult Pornography, Child pornography which includes pornographic materials involving minors and other sexually suggestive materials escort or prostitution services; Website access and / or website memberships of pornography or illegal sites.

8. Gambling and Gaming

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

9. Hacking, Cracking, Cheating and Forgery

Hacking and cracking materials which include manuals, how-to guides information, or equipment enabling illegal access to software, servers, watomites, or other protected property Bulk email software or Bulk marketing tools or Multilevel marketin enabling unsolicited messages (spam) or for collection of fees or Work-at- home approach

10. Offensive/Crime Goods

Offensive goods, which includes literature, products or other materials that.

a) Defame or slander any person or groups of people based or race, ethnicity, national origin, religion, sex, or other factors
b) Encourage or incite violent acts
c) Promote intolerance or hatred

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

11. Currency, Exchanges and Financial Products and Services

Discounted currencies or unauthorized currency exchanges; Securities, which includes stocks, bonds, or related financial products ; Investment in crypto currencies, including bitcoin.

12. Foreign Contributions, Political Funding, Hawala Transactions

Foreign Contributions, which are regulated through FCRA, 1976; Political Funding/ Contributions to any recognized / unrecognized Political Party; hawala transactions.

13. Others

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.

Part - II : Prohibited transactions

1. Acceptance of transactions in violation of KYC/AML guidelines.
2. Processing transactions to cover previously incurred debts, or bad debts such as bounced cheque/s, or payment for returned merchandise.
3. Processing a sale on a previously charged back transaction.
4. Using a split sale to avoid authorization requirements.
5. Delivering goods or performing services after notice of a cancellation by the cardholder of a pre-authorized order.
6. Billing card after notice of cancellation of recurring payment, if any.

Annex-ll: Indicative list of avoidable Merchants through Payment Gateway/ Aggregators

a) Telephone Based Selling (also called Audio-Text) This involves high- pressure selling tactics/ exaggerations and often false promises.

b) Timeshares: Very long fulfillment period.

c) Pyramid Selling/Multi-Level-Marketing Companies: High Pressure selling techniques can result in customer dissatisfaction, resulting in disputes/Chargebacks.

d) Dating/Escort Agencies: Customers can Chargeback transactions due to unhappiness with quality of introductions.

e) Betting/Gambling/Lotteries/Games of Chance/Sweepstakes: Restrictions by RBI.

f) Health Elixir Sales/Beauty & lifestyle products/Beauty therapies and parlors offering the same: Exaggerated claims of beauty, reversal of age. attainment of youthfulness etc. These services/ products are very personal in nature, and are not quantifiable, thus leading to cardholder dissonance and disputes.

g) Massage Parlors: Often conduct unethical/ unlawful businesses, which can damage the Acquirer's reputation by implication.

h) Merchants dealing in lllegal/ unlawful Merchandise Examples include pet shops which deal in trading of endangered/ protected birds/animals Merchants dealing in Pornographic or the so-called Adult/Mature material also fall under this category.

i) Intangibles Example of this includes software downloaded via the Internet. In case of Chargebacks, it is often very difficult to prove that the Software could be downloaded and installed successfully/correctly by the user.

j) Non-Government Organizations (NGO)

k) Political Parties

Note: Branches are required to do due-diligence while selecting merchant and it should be responsibility of the branches not to select merchant from avoidable Merchant Categories

Annex-All: Indicative IT security Requirements for adoption By the Payment Aggregators and Payment Gateways

Security-related Requirements

The mandatory requirements for Payment Aggregator and recommended requirement for Payment Gateway in respect of IT systems and security are as under.-

1.1. Infrastructure: The entities shall have IT infrastructure at both Data Centre and Disaster Recovery Centre. AII IT assets should be under warranty AMC Business Continuity Plan and Business Continuity Management must be in place. Minimum availability of 99% is to be ensured, by putting in place appropriate hardware, software, network and other related components

1.2. Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment to identify risk exposures with remedial measures and residual risks These can be internal security audit and annual security audit by an independent security auditor or a CERT-An empanelled auditors. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board. Payment Gateways and Aggregators shall comply with Bank's Information Security Policy/guidelines, as amended from time to time.

1.3. Data Security Standards: Data security standards and best practices hike PC- DSS, PA-DSS, latest encryption standards, Transport Channel Security etc. shall be implemented.

14. Security Incident Reporting: The entities shall report security incidents / card holder data breaches within timeframe to Bank/relevant authorities. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall also be submitted to relevant stakeholders

15. Merchant Onboarding The entities shall undertake comprehensive security assessment during merchant onboarding process to ensure these minimal baseline security controls are adhered to by the merchants

1.6. Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment/Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective/preventive actions planned with action closure date; Inventory of applications which stores or processes or transmits customer sensitive data; PA.DSS compliance status of payment applications which stores or processes card holder data.

1.7. Information Security: Board approved Information Security Policy shall be reviewed at least annualy.

1.8. IT Governance: An IT policy needs to be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented The Board level IT Governance framework of Payment Aggregators shall have,

a) Involvement of Board. The major role of the Board/Top Management shall involve approving information security policies, establishing necessary organizational processes/ functions for information security and providing necessary resources.

b) IT Steering Committee: An IT Steering Committee shall be created with representations from various business functions as appropriate. The Committee will assist the Executive Management in the implementation of the IT strategy approved by the Board. It shall have well defined objectives and actions.

c) Enterprise Information Model The entities shall establish and maintain an enterprise information model to enable applications development and decision supporting activities, consistent with board approved IT strategy. It shall facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure.

d) Cyber Crisis Management Plan. The entities shall prepare a comprehensive Cyber Crisis Management plan and approved by IT strategic committee and shall include components such as Detection, Containment, Response and Recovery.

1.9. Enterprise Data Dictionary. The entities shall maintain an enterprise data dictionary incorporating organization's data syntax rules. This should enable the sharing of data among applications and systems, promote a common understanding of data among tT and business users and preventing creation of incompatible data elements

1.10. Risk Assessment The risk assessment must, for each asset within its scope, identify the threat/ vulnerability combinations and likelihood of impact on confidentiality, availability or integrity of that asset - from a business, compliance and/or contractual perspective.

1.11 Access to application. There shall be documented standards / procedures for administering an application system, which are approved by the application owner and kept up-to-date Access to the application shall be based on the principle of least privilege and "need to know commensurate with the job responsibilities

1.12. Competency of Staff: Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately with a periodic assessment of the training requirements for human resources.

1.13. Vendor Risk Management : The Service Level Agreements (SLAs) for technology support, including BCP.DR and data management shall categorically include clauses permitting regulatory access to these set-ups.

1.14. Maturity and Roadmap: The entity shall consider assessing their IT maturity level, based on well-known international standards, design an action plan and implement the plan to reach the target maturity level.

1.15. Cryptographic Requirement. Entities shall select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.

1.16. Forensic Readiness: All security events from entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts

1.17 Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorized access to the data.

1.18. Data Security in outsourcing: There shall be an outsourcing agreement providing 'night to audit' clause to enable entities / their appointed agencies and regulators to conduct Security audits. Alternatively, third party to submit annual independent security audit report to entities.

1.19. Payment Application Security: Payment applications shall be developed as per PA-DSS guidelines and complied with as required. The entities shall review PCIDSS compliance status as part of merchant onboarding process.

S.No.	Checklist	Complied
1	Request proposal from Payment Aggregator	Yes/No
2	PCIDSS Compliance and license from RBI	Yes/No
3	Complies the regulations under companies act 1956/2023	Yes/No
4	Authorization from RBI under the Payment and Settlement Systems Act, 2007 (PSSA).	Yes/No
5	The Memorandum of Association (MoA) of the entity must cover the activity of operating as a Payment Gateway and Payment Aggregator	Yes/No
6	Review of PG/PA on various aspects on annual basis	Yes/No
7	Cross border transaction through AD Category Branches should be guide through RBI's foreign transaction guidelines	Yes/No
8	Proper Due diligence, Market report, financials, credibility should be checked before empanelment	Yes/No
9	Appointment of Nodal officer, Relationship Manager, proper grievance redressal mechanism by Pas.	Yes/No
10	Pas shall have a Board approved policy for merchant on-boarding inclusively KYC norms, Website compliance, customer privacy and return policy etc.	Yes/No
11	Settlement of transaction within time frame with transparency on transaction entries. Adequate balance on escrow accounts should be checked periodically.	Yes/No
12	List of prohibited goods, transactions and list of avoidable Merchant should be checked before onboarding Merchant.	Yes/No