Reserve Bank of India
Department of Payment and Settlement Systems

Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators

Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators

1. Background

1.1 Payments in the online space are facilitated by a number of intermediaries like the payment gateways and payment aggregators. These intermediaries act as the bridge between the providers of goods / services (merchants) and those that require them (customers). For a successful online experience, the role of such intermediaries is crucial.

1.2 The intermediaries involved in payment collection and settlement between customers and merchants range from banks providing payment gateway services, non-bank aggregators of merchants and payment options / instruments, technology service providers supporting payment gateway operations and e-commerce marketplaces.

1.3 Extant regulation in this area, albeit indirect, were issued by Reserve Bank of India (RBI) during November 2009 which required banks to maintain a nodal account of the intermediaries with permissible credits and debits as also the settlement cycle for credit to the merchants. This nodal account was required to be in the form of an 'internal account' of the bank.

1.4 The instructions were motivated with a view to safeguard the interests of the customers and users and to ensure that the payments made by them using electronic / digital / online payment modes were duly accounted for by the intermediaries receiving such payments and transmitted to the accounts of the merchants or to similar other entities.

1.5 There have been no changes to these guidelines since its issue. Payment Systems in India have witnessed rapid changes in the last decade. The facilitating role of innovation, fintech, expanding e-commerce activities, etc., has contributed to the impressive growth. In this fast-changing scenario, it is opportune to review if the extant guidelines / regulatory prescriptions are adequate. It is also time to see if a regime of direct regulation is warranted.

1.6 In its Monetary Policy Statement for 2018-19 dated February 7, 2019, RBI had indicated that the existing guidelines for Payment Intermediaries would be reviewed. This discussion paper covers the various facets of the activities of the Payment Gateways and Payment Aggregators and presents different options towards their regulation.

2. Payment Gateways and Payment Aggregators

2.1 In an online payment transaction, the following entities / players are generally involved – seller (merchant), customer (buyer), customer's bank / wallet account, acquiring bank, the bank having the nodal account, IT and communication hardware / software, middleware, security systems, payment gateways and payment aggregators. The means opted for payment could be a credit card, debit card, bank account, wallet, Unified Payments Interface (UPI), etc. Depending on the payment mode used, additional players like card networks, NPCI (National Payments Corporation of India), banks offering net-banking services, banks / non-banks issuing wallets, etc. may be part of the payment chain.

2.2 Payment Gateways and Payment Aggregators refer to entities who –

a) provide technology infrastructure to route and / or facilitate processing of an online payment transaction and perform other functions without actually handling the funds.

b) facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations to the merchants

without the need for merchants to create a separate payment integration system of their own.

c) facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer them on to the merchants after a time-lag. Apart from handling funds, they also get access to customer data.

2.3 Payment Gateways and Payment Aggregators may also provide services which include generation of settlement via netting of the funds received by the merchants onboarded by them. By being the bridge between consumers at one end and merchants at the other end, these service providers play a role in processing and completion of the payment transactions. They could be engaged by a bank, a merchant, or a biller (utility company, telco, etc.).

2.4 Payment Gateways and Payment Aggregators engaged by a bank: Payment Gateways and Payment Aggregators may be engaged by a bank to enable the latter to provide its customers services like bill payments, card payments, etc. – across its various banking channels and through use of cards / bank accounts. Such aggregators generally (i) provide the technology interface for the services, (ii) enter into arrangements with biller / utility entities, (iii) manage the daily operational complexities of dealing with multiple utilities (each with a disparate technology platform) in different locations, (iv) provide the banks one standardised – centralised manner of dealing with the bill-data of various utilities, (v) take care of various biller / utility requirements of MIS, reconciliation, consolidated pay outs and other service delivery aspects, etc.

2.5 Payment Gateways and Payment Aggregators engaged by a merchant / biller: Merchants may also engage Payment Gateways and Payment Aggregators to provide transaction management / consolidation services for managing collections / payments through various payment modes. This normally includes (i) online transaction processing across various banks / card 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.

2.6 Currently most of acquiring is done by third party aggregators and technology providers. There, entities may also provide cross border settlement services and are governed by guidelines issued by Foreign Exchange Department (FED, RBI) on Online Payment Gateway Service Providers (OPGSPs).

3 Concerns and Gaps

3.1 The activities of Payment Gateways and Payment Aggregators in online transactions are extremely crucial. Entities may be a source of risk in such a technology and customer experience intensive business if they have inadequate governance practices which may impact customer confidence and experience.

3.2 The customer, ordinarily has very limited access to the Payment Gateways and Payment Aggregators and must rely on merchants or banks who only can seek redress from the Payment Aggregators. Lack of proper redress mechanism and uniformity in practice across the entities is also a matter of concern.

3.3 It is however a fact that the present guidelines of indirect regulation of such intermediaries (through the nodal banks) has withstood the test of time. Over the last 10 years, no major complaints have been received on this arrangement.

3.4 Furthermore, there is need for appropriate delineation of roles and responsibilities among merchants and customers, clarity in case of routing of transactions through proper reporting of transactions handled, etc. Being part of the payments process chain these entities also handle sensitive customer data. Managing customer data, data privacy, Know Your Customer (KYC) requirements of merchants are also important from the point of view of security and customer confidence in the ecosystem.

3.5 The technology set-up of Payment Gateways and Payment Aggregators varies amongst the entities and the architecture changes over time keeping in view their predominant business objective including the need to provide efficient processing, seamless customer experience, etc. They may resort to multiple integration to provide redundancy.

3.6 Leveraging their market presence, some of the e-commerce market places also offer payment aggregation services. The primary business of these e-commerce marketplaces does not come within the regulatory ambit of RBI and in case of regulatory prescriptions for payment Aggregators, they would end up being subjected to dual regulation. Hence, a separation of these two activities would entail a better regulatory approach / process.

3.7 The existing regulations are applicable to intermediaries who collect monies from customers for payment to merchants using any electronic / online payment mode. Thus, essentially, transactions reflecting pay-ins by the aggregators to the merchants are included (i.e. debit transactions).

4. Regulatory Approaches / Options

Based on the understanding of the current ecosystem, certain regulatory options and approaches are suggested in this discussion paper for regulating the activities of Payment Aggregators and Payment Gateways.

4.1 Option 1 : Continue with the extant instructions with minor changes in respect of definition of 'T' and clarify the applicability of the guidelines.

4.2 Option 2 : Limited Regulation : The Payment Gateways and Payment Aggregators shall follow the norms and guidelines in respect of minimum net-worth, merchant on-boarding, timelines for settlement of funds, maintenance of escrow account, IT security, etc., and shall be required to submit certain returns to RBI. The Payment Gateways and Payment Aggregators to be licensed / registered in a phased manner, over a period of time. Only off-site monitoring would be resorted to.

4.3 Option 3 : Full and Direct Regulation

4.3.1 Payment Gateways and Payment Aggregators shall be authorised under the Payment and Settlement Systems Act, 2007 (PSSA). Sufficient time, of say one year, may be given to the existing market participants to achieve compliance with the required capitalisation norms. They shall adhere to the regulations from the date of issue of the regulations or as specified therein. Further, the authorised Payment Gateways and Payment Aggregators shall also, if required, maintain the funds received from customers in an escrow account with a scheduled commercial bank.

4.3.2 These entities shall be subjected to both on-site and off-site monitoring. A brief of requirements under direct regulation is given below (details in Annex 1) :

i. Authorisation / Licencing : The regulations would be applicable to Payment Aggregators and Payment Gateways. Non-bank Payment Aggregators and Payment Gateways shall require authorisation from RBI under PSSA. Entities undertaking Payment Aggregation and Payment Gateway activity shall be a company incorporated in India under the Companies Act, 2013. They shall be given one financial year (from date of issue of guidelines) to comply with the entry point norms and other technology, security, storage, etc., norms issued in this regard.

ii. Capital Requirements : Capital requirements shall have minimum net-worth as prescribed for Bharat Bill Payment Operating Unit (BBPOUs) (currently ₹ 100 crore) to be maintained at all times. Existing Payment Aggregators shall, within one year after the issuance of guidelines by RBI, comply with this net-worth requirement. Entities not able to comply with the net-worth requirement within the stipulated time frame, need not apply for authorisation but shall wind-up payment aggregation business within one year of issuance of guidelines.

iii. Governance : The entity shall be professionally managed where the promoters of the company shall satisfy the fit and proper criteria prescribed by RBI. There shall be a Board approved policy for disposal of complaints / dispute resolution mechanism / time-lines for processing refunds, etc. Entities shall appoint a Nodal Officer responsible for regulatory and customer grievance handling functions whose details are prominently displayed on their website.

iv. Safeguards against Money Laundering (KYC / AML / CFT) Provisions : 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 apply *mutatis mutandis* to all the Payment Aggregators and Payment Gateways along with the provisions of Prevention of Money Laundering Act, 2002 and Rules framed thereunder, as amended from time to time.

v. Customer Grievance Redressal and Dispute Management Framework : Payment Aggregators shall put in place a formal, publicly disclosed customer grievance redressal framework and dispute management framework, including designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution. The customer and the merchant complaints shall be promptly handled / disposed of by the Payment Aggregators and Payment Gateways as per their Board approved policy, within a period of 7 working days of receipt of complaint by the Payment Aggregator.

4.3.3 As banks are already regulated entities of RBI, the Payment Gateway services provided by them need not require a separate authorisation as these activities form part of regular banking business. They shall, however, comply with other prescriptions regarding time-lines, customer grievance redressal mechanism, etc. However, where the banks act as Payment Aggregator they have to obtain authorisation under PSSA.

4.3.4 Payment Gateways and Payment Aggregators, if found to be operating without obtaining authorisation from RBI shall be penalised as per provisions under the PSSA.

5 Coverage of Framework

5.1 The framework will cover :

a) The activities of Payment Gateways and Payment Aggregators in online transactions, their capital requirements, governance, safeguards against money laundering (KYC / AML / CFT) provisions, merchant on-boarding, settlement and escrow account management, customer grievance redressal & dispute management framework, security, fraud prevention and risk management framework, Information System Audit, etc.
b) The technological prescriptions for Payment Gateways and Payment Aggregators.

5.2 The framework will not cover :

a) Intermediaries who facilitate delivery of goods / services immediately / simultaneously (e.g. travel tickets / movie tickets, etc.) on the completion of payment by the customer i.e., where the delivery is linked to completion of corresponding payment.
b) Cash on Delivery (CoD) e-commerce model and processing and settlement of import and export related payments facilitated by OPGSPs who are guided by instructions issued by FED, RBI.
c) e-commerce marketplaces collecting payments for various merchants for transactions in respect of goods and services sold on their platform.
d) Other bilateral arrangements of merchants with the aggregators to consolidate and make payments to vendors, agents, etc.

6 Principles / Basis for Regulation

6.1 Payment Gateways and Payment Aggregators are a critical link in the transaction flow and there is a case to regulate activities and these fall within the ambit of PSSA.

6.2 The Payment Gateway services of banks also involves activities similar to non-bank Payment Aggregators. However, since the funds being managed on behalf of the merchants are a part of their banking relationship and the merchants have other safety nets to have recourse vis-à-vis the banks, their activities cannot be equated with that being done by non-bank Payment Aggregators. There is, however, merit in banks providing Payment Gateway services to also adhere to the minimum technical requirements.

6.3 In maintaining a nodal account, as an internal account with a bank, there is no beneficial interest being created on such accounts on behalf of the intermediary and / or merchants. Further, these accounts are a liability of the bank thus do not form part of the balance sheet of the Payment Aggregator. The fund management need, therefore, to be through an escrow account arrangement with or without a tri-partite agreement including some return on core portion as in case of PPI regulations. Section 23A of the PSSA provides protection to the funds collected from customers and maintained in escrow accounts with banks. This benefit will also be available if the prescribed approach is shifted from nodal account with banks to the escrow with banks.

Annex 1

Regulatory Prescriptions / Specifications for Full and Direct Regulation

(Applicable only if Option 3 is exercised)

1 Authorisation / Licencing

1.1 The regulations would be applicable to Payment Gateways and Payment Aggregators.

1.2 Non-bank Payment Gateways and Payment Aggregators shall require authorisation from RBI under PSSA.

1.3 Existing Payment Gateways and Payment Aggregators shall apply for authorisation; however, they shall be given one financial year (from date of issue of guidelines) to comply with the entry point norms and other technology, security, storage, etc. norms issued in this regard.

1.4 E-commerce marketplaces acting as Payment Gateways and Payment Aggregators to other merchants shall stop the activity within 3 months. If they desire to pursue this activity, it shall be separated from marketplace business and the separate entity shall comply with the regulations.

1.5 Banks acting as Payment Gateways and Payment Aggregators shall obtain authorisation / approval under PSSA along with a 'No Objection Certificate' from the respective regulatory department of RBI.

1.6 Entities undertaking Payment Gateways and Payment Aggregators activity shall be a company incorporated in India under the Companies Act, 2013.

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

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

2 Capital Requirements

2.1 Capital requirements shall have minimum net-worth as prescribed for Bharat Bill Payment Operating Unit (BBPOUs) to be maintained at all times (currently ₹ 100 crore). Existing Payment Gateways and Payment Aggregators shall, within one year after the issuance of guidelines by RBI, comply with this net-worth requirement.

2.2 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.

2.3 Entities having Foreign Direct Investment (FDI) / Foreign Portfolio Investment (FPI) / Foreign Institutional Investment (FII) shall also meet the capital requirements as applicable under the extant Consolidated FDI policy guidelines of Government of India.

2.4 Entities not able to comply with the net-worth requirement within the stipulated time frame, need not apply for authorisation but shall wind-up payment aggregation business within one year of issuance of guidelines. The banks presently maintaining nodal accounts of such entities shall have to report compliance in this regard.

3 Governance

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

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

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

3.4 The entity shall have a Board approved policy for disposal of complaints / dispute resolution mechanism / time-lines for processing refunds etc.

3.5 The entity shall appoint a Nodal Officer responsible for regulatory and customer grievance handling functions. Details of the nodal officer should be prominently displayed on their website.

4 Safeguards against Money Laundering (KYC / AML / CFT) Provisions

4.1 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 apply mutatis mutandis to all such entities.

4.2 Provisions of Prevention of Money Laundering Act, 2002 and Rules framed thereunder, as amended from time to time, shall also be applicable.

5 Definitions

5.1.1 The definitions considered in this discussion paper are elucidated in the Glossary provided at the end.

5.1.2 Time lines:

- ✓ '**T**' is the date and time of charge / debit to the customer's account used for making payment for purchase of goods / services.
- ✓ '**Ts**' is the date and time of intimation by the merchant to the Intermediary (aggregator / marketplace) about shipment of goods.
- ✓ '**Td**' is the date and time of confirmation by the merchant to the Intermediary (aggregator / marketplace) about delivery of goods to the customer.

6 Merchant On-boarding

6.1 The Payment Gateways and Payment Aggregators shall ensure compliance to KYC/AML requirements while onboarding merchants. 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, do not sell fake / counterfeit / prohibited products, etc. The merchant's website shall clearly indicate the terms and conditions of the service and time-line for processing returns and refunds.

6.2 The entity shall undertake due diligence, inter-alia, through checking merchant website for authenticity and security purposes. The approach shall not be of merely obtaining a self-assessment / declaration from the merchant as sufficient process for onboarding a merchant.

6.3 As and when required, the entity shall demonstrate and prove that there was no compromise in the process of due diligence. In addition, technical aspects like internet traffic, information disclosure policy, digital footprint, privacy policy, etc., shall also be checked.

6.4 The contract signed with the merchant by the payment aggregator shall clearly indicate that the merchant cannot act as a sub-aggregator and shall route transactions pertaining only to his / her own business.

6.5 While on-boarding merchants, such an entity shall comply with the requirements, if any, issued by any other regulator and / or any payment instrument provider regarding not permitting certain businesses from accepting electronic payments.

6.6 The entity shall be responsible to check that the infrastructure of the merchant deployed for connecting to the aggregator is PCI-DSS (Payment Card Industry-Data Security Standard) and PA-DSS (Payment Application Data Security Standard) complaint. Merchant's infrastructure storing customer payment data should be PCI-DSS compliant on an on-going basis. Merchant site should not perforce save the customer card, and such related data. The customer should be given the consent option and the default option should be 'NO'. If required a security audit of the merchant may be carried out before on boarding.

6.7 The agreement with merchant shall have provision for security / privacy of customer data. The agreement with merchants shall include compliance to PCI - 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.

7 Customer Grievance Redressal & Dispute Management Framework

7.1 Payment Gateways and Payment Aggregators shall put in place a formal, publicly disclosed customer grievance redressal framework and dispute management framework, including designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution. The complaint facility, made available on website / mobile, shall be clearly and easily accessible.

7.2 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.

7.3 The Payment Gateways and Payment Aggregators shall disclose comprehensive information regarding merchant policies, pricing, customer grievances, privacy policy and other terms and conditions on the website and / or their mobile application.

7.4 The Payment Gateways and Payment Aggregators shall 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 them, compliance, responsibilities of

all the parties, documentation, reason codes, procedure for addressing the grievance, turn-around-time for each stage, etc.

7.5 If the goods / services are not delivered to the customer within the time-lines as conveyed by the merchant to the customer, the Payment Gateways and Payment Aggregators shall protect their own interest by having necessary recourse clauses in the agreements signed and / or obtaining guarantee / funding of risk reserve by the merchant.

7.6 The customer including the merchant complaints shall be handled / disposed of by the Payment Gateways and Payment Aggregators within such time and in such manner as provided for in its Board approved policy, but in any case not beyond a period of 7 working days of receipt of complaint by the Payment Aggregator.

8 Security, Fraud Prevention and Risk Management Framework

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

8.2 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 Annex 2 for adoption by the Payment Aggregator and Payment Gateways.

8.3 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 immediately to DPSS, RBI, Central Office, Mumbai and CERT-In (Indian Computer Emergency Response Team) as per the details notified by CERT-In.

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

8.5 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 respective Regional Office of DPSS, RBI.

9 Reports

9.1 The reports to be submitted by authorised Payment Gateways and Payment Aggregators, as applicable are listed in Annex 3.

10 General Instructions

10.1 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.

10.2 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.

10.3 The Payment Gateways and Payment Aggregators shall not invoke ATM PIN as a factor of authentication for card not present transactions involving debit card transactions.

10.4 The Instructions on storage of payment system data as applicable to PSOs would apply to the authorised Payment Gateways and Payment Aggregators.

Annex 2

IT Security Issues

Indicative IT security recommendations for adoption by the Payment Aggregators and Payment Gateways are:

1. Security-related Recommendations

1.1. The baseline and desirable requirements for payment aggregators in respect of IT systems and security are presented below.

1.1.1. Base line Requirements.

(i) 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-In empanelled auditors. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.

(ii) Data Security Standards: Data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, Transport Channel Security etc. shall be implemented.

(iii) Security Incident Reporting: The entities shall report security incidents / card holder data breaches within 2-6 hours timeframe to RBI. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall also be submitted to RBI.

(iv) 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.

(v) 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.

1.2. Desirable Requirements

(i) Information Security: Board approved Information security policy shall be reviewed at least annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organizational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classifications; authorization; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.

(ii) 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 strategic plan and policy shall be reviewed annually. 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.

(iii) 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 IT and business users and preventing creation of incompatible data elements.

(iv) 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.

(v) 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.

(vi) 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.

(vii) Vendor Risk Management: Practices shall be followed by payment aggregators when engaging with TSPs. The Service Level Agreements (SLAs) signed by Payment Aggregators for technology support, including BCP-DR and data management shall categorically include clauses permitting regulatory access to these set-ups.

(viii) Maturity and Roadmap: The Payment Aggregators 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.

(ix) Cryptographic Requirement: Payment Aggregators 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.

(x) Forensic Readiness: All security events from Payment Aggregator’s 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.

(xi) Data Sovereignty: The Payment Aggregators 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.

(xii) Data Security in outsourcing: There shall be an outsourcing agreement providing 'right to audit' clause to enable Payment Aggregators / their appointed agencies and regulators to conduct Security audits. Alternatively, third party to submit annual independent security audit report to Payment Aggregators.

(xiii) Payment Application Security: Payment applications shall be developed as per PA-DSS guidelines and complied with as required. Payment Aggregators to review PCI-DSS compliance status as part of merchant onboarding process.

(xiv) Security Incident Reporting: Cyber Security incidents shall be reported by Payment Aggregators to regulator within 2-6 hours duration. Payment Aggregators to bind merchants on security incident reporting through agreements.

Annex 3

Reports to be submitted by Authorised Payment Aggregators

Annual

1. Audited Annual report with CA certificate on Networth – by September 30th.
2. IS Audit Report and Cyber Security Audit Report with observations noted, if any, including corrective / preventive action planned with closure date – Externally Audited – by May 31st.
3. Networth Certificate as on September 30th (un-audited) on self-declaration basis – by December 31st.

Quarterly

1. Auditors' Certificate on Escrow Balance – by 15th of the month following the quarter end.
2. Bankers' Certificate on Escrow Account Debits and Credits – Internally Audited – by 15th of the month following the quarter end.
3. Auditors' Certificate on Nodal Accounts – for Marketplaces – by 15th of the month following the quarter end.
4. Customer Grievances Report – by 15th of the month following the quarter end.
5. Cyber Security Audit Report – Internally audited – by 15th of the month following the quarter end.

Monthly

1. Statistics of transactions handled – by 7th of next month.
2. Report on frauds – by 7th of next month.
3. Cyber Security incident reports – with root cause analysis and preventive action undertaken – by 7th of next month.

Non-periodic

1. Technical Audit – one time; also as and when a major change is made to process flow.
2. Change in Board of Director – as and when happens.

Abbreviations

ATM	Automated Teller Machine	MIS	Management Information System
BBPOU	Bharat Bill Payment Operating Unit	MoA	Memorandum of Association
BBPS	Bharat Bill Payment System	NACH	National Automated Clearing House
BCP	Business Continuity Plan	NPCI	National Payments Corporation of India
BPSS	Board for (Regulation and Supervision of) Payment & Settlement Systems	OPGSP	Online Payment Gateway Service Provider
CERT-In	Indian Computer Emergency Response Team	PA	Payment Aggregator
CoD	Cash on Delivery	PA-DSS	Payment Application-Data Security Standard
DIPP	Department of Industrial Policy and Promotion	PAN	Permanent Account Number
DPSS	Department of Payment and Settlement Systems	PCI	Payments Council of India
DR	Disaster Recovery	PCI-DSS	Payment Card Industry-Data Security Standard
DSS	Data Security Standard	PFMI	Principles for Financial Market Infrastructures
EMI	Equated Monthly Instalment	PG	Payment Gateway
EU	European Union	PIN	Personal Identification Number
FDI	Foreign Direct Investment	PoS	Point of Sale
FED	Foreign Exchange Department	PPI	Prepaid Payment Instrument
FII	Foreign Institutional Investment	PSSA	Payment & Settlement Systems Act, 2007
FPI	Foreign Portfolio Investment	PTS	PIN Transaction Security
GoI	Government of India	RBI	Reserve Bank of India
HR	Human Resource	ReBIT	Reserve Bank Information Technology Pvt. Ltd.
IS	Information Security	RO	Regional Office
IT	Information Technology	SLA	Service Level Agreement
KYC	Know Your Customer	TSP	Technology Service Provider
MID	Merchant Identification	UPI	Unified Payments Interface

Glossary

Bharat Bill Payment System (BBPS)	A one-stop payment platform for bills of utility agencies providing an interoperable and accessible bill payment service to all customers across India. The system provides customers with the option to pay any bill anytime and from anywhere.
Board for (Regulation and Supervision of) Payment and Settlement Systems (BPSS)	The sub-committee of the Central Board of the Reserve Bank of India, is an apex policy making body on payment systems in the country. The BPSS is empowered to authorize, prescribe policies and set standards for regulating and supervising the payment and settlement systems in the country.
Customers	Buyers / Beneficiaries of goods and services from a merchant who have routed their payment for the purchases through an electronic / online payment platform. The customers may / may not be aware of the role, presence or involvement of the online payment service provider.
E-commerce[1]	Buying and selling goods and services including digital products over digital and electronic networks, which may have – - Inventory based model of e-commerce where inventory of goods and services is owned by e-commerce entity and is sold to the consumers directly. - Marketplace model of e-commerce which involves providing an IT platform / digital / electronic network to act as a facilitator between the buyer and seller.
Financial Market Infrastructures (FMI)	Generally refers to systemically important payment systems, Central Securities Depositories (CSDs), Securities Settlement Systems (SSSs), Central Counter Parties (CCPs), and Trade Repositories (TRs) that facilitate the clearing, settlement, and recording of financial transactions. FMI is a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.
Merchants	Includes any domestic entity which accepts payments, through an electronic / online payment platform, for goods and services offered by them. Merchants may have connectivity with multiple payment aggregators as per their business requirements and / or, inter-alia, for redundancy.
Payment Aggregator (PA)	An intermediary in an online payment transaction accepting payments on behalf of the merchant from the customers and then transferring the money to the merchant's account.

[1] DIPP, GoI, Press Note 2 (2018 series) - DIPP (Department of Industrial Policy and Promotion), GoI guidelines indicate that e-commerce marketplace may provide support services including for payment collection and these may facilitate payments for sale in conformity with the guidelines of RBI.

Payment Gateway (PG)	A technology infrastructure provider to route and facilitate processing of an online payment transaction, without any involvement in the actual handling of funds.
Payment System (PS)	A system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. Payment system includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations.[2]
Payment Card Industry - Data Security Standard (PCI-DSS)	A set of security standards designed to ensure that all companies that accept, process, store or transmit card information maintain a secure environment.
Payment Application Data Security Standard (PA-DSS)	A security standard for software vendors that develop payment applications. The standard aims to prevent storage of prohibited secure data (CVV2, PIN magnetic stripe).
Payment Gateway services provided by banks	Includes services provided by banks for facilitating collection of electronic payments for the merchants on boarded by them. Such a bank credits the monies received on behalf of a merchant for such transactions into the current account of the merchant opened with that bank like any other routine banking operations.
Payment Gateway services provided by non-banks	Non-banks provide technology services to various entities by routing the transactions emanating from the merchant's site to the customer's account and the merchant's bank account.
Personal Identification Number (PIN)	A numerical code ranging from 3 to 6 digits to be used by a card holder in online electronic financial transactions and generally in conjunction with user-name and / or other passwords. The PIN can be static (same for every transaction) or dynamic (different for every transaction).
Payment and Settlement Systems Act, 2007 (PSSA)	A legislation that provides for regulation and supervision of payment systems in India and designates the Reserve Bank of India as the authority for the purpose.
Technology Service Providers	Includes entities providing only technology platform or support (software, hardware or a technical service) to bank payment gateways, non-bank payment aggregators, e-commerce platforms, etc. Being pure technology service providers, they do not at any point hold the monies transacted between the customer and merchant.
Nodal Account	It is an internal account of the bank, opened for facilitating collection of payments by intermediaries from customers of merchants.
Escrow Account	Account maintained in a bank in which funds are held for specific credits and debits.

[2]Section 2 (1) (i) of PSSA