Sep 2020

India: Payments in e-commerce sector set for a new innings

The Indian e-commerce space has garnered a significant consumer base in the past decade, accelerated by the ongoing global Coronavirus pandemic. Users have shifted to digital modes of transactions (including credit and debit cards, and various mobile payment modes), with the volume soaring to around 100 million daily transactions on average. In a development that is set to revamp the e-commerce space in India, RBI issued 'Guidelines on Regulation of Payment Aggregators and Payment Gateways[1]' ('the Guidelines'), dated 17 March 2020, which came into effect on 30 September 2020[2]. Sanjana Rao, Aaron Kamath, and Vivek Kathpalia, from Nishith Desai Associates, provide an overview of the Guidelines, looking particularly at payment aggregators and payment gateways, as well as the future of the e-commerce sector in India.

MicroStockHub / Signature collection / istockphoto.com

The Reserve Bank of India ('RBI'), the country's central bank, predicts that digital payments will jump to 1.5 billion transactions (worth INR 1.5 trillion (approx. €17 billion)) a day in the next five years[3]. Data released by the RBI also shows that amounts aggregating to approximately INR 954 billion (approx. €11 billion) through card payments[4] and approximately INR 6.3 trillion (approx. €73 billion) through mobile transactions[5], were transacted in the month of July 2020. Overall, as can be seen from statistics alone, India is understandably a prime destination for e-commerce and FinTech players.

New law for electronic payment service providers

The Guidelines prescribe that 'payment aggregators' will need to obtain an authorisation from the RBI to operate, though no authorisation is required for 'payment gateways.' The Guidelines prescribe certain technology and security-related recommendations that are mandatory for payment aggregators, and recommendatory for payment gateways.

Prior to the Guidelines, payment service providers who facilitated electronic payments between users and online merchants were classified as 'intermediaries.' Intermediaries were regulated under the RBI's 'Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries[6]' ('the 2009 Directions'), dated 24 November 2009. There was no licensing regime for intermediaries under the 2009 Directions and instead, intermediaries were indirectly regulated by the RBI via the banks that they were involved with. The Guidelines are expected to replace the regime under the 2009 Directions in a phased manner.

New concept of payment aggregators and payment gateways

The Guidelines provide for new concepts of 'payment aggregators' and 'payment gateways.' Whilst the former is subject to authorisation and ongoing compliance requirements, the latter largely remains unregulated and subject to recommendatory, though not mandatory, technology and security-related practices.

Payment aggregators

Payment aggregators have been described under the Guidelines to mean entities which, 'facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own.

Payment aggregators are essentially those service providers that facilitate payments to merchants, and that receive, pool and transfer user payments to the merchants as part of the facilitation process.'

The RBI considered the need for a formalised licensing regime for payment aggregators initially in its discussion paper dated 17 September 2019[7]. In this discussion paper, the RBI noted that, '[f]or a successful online experience, the role of such intermediaries is crucial... 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 appears that the RBI has taken the approach towards full and direct regulation of such market players.

Existing payment aggregator entities are required to apply for an authorisation on or before 30 June 2021 and achieve net-worth of INR 150 million (approx. €1.7 million) latest by the date of their application or 31 March 2021, whichever is earlier. Subsequent requirement of achieving net-worth of INR 25 million (approx. €290,000) will have to be met over a subsequent 3-year period. New entities which seek to commence activities of a payment aggregator appear to require an authorisation from the RBI prior to doing so.

Payment gateways

Payment gateways, on the other hand, have been described to mean entities which provide 'technological infrastructure to route and facilitate processing of an online payment transaction without their own involvement in handling of funds.' Given that there is no handling of funds by a payment gateway, they have been exempted from obtaining a specific RBI authorisation to carry on their activities.

Technology and security-related recommendations

- Certain baseline technology and security-related recommendations have been set out under the Guidelines. The recommendations are mandatory for payment aggregators, though not for payment gateways. Payment aggregators are required to have in place a strong risk management system, and data security infrastructure, necessary to meet the challenges of fraud and ensure customer protection.
- Payment aggregators are to ensure that merchants are PCI-DSS and PA-DSS compliant and the agreements with merchants should provision for security and privacy of customer data.
- Payment aggregators should ensure that merchants do not store customer card and related data. Payment aggregators should not store customer card credentials within their data-base or the server accessed by the merchant. They are also required to comply with data storage requirements including data localisation norms prescribed by the RBI.

- The payment aggregators are also required to establish a mechanism for monitoring, reporting, handling, and following-up of cybersecurity incidents and breaches.
- A System Audit Report, including a cybersecurity audit conducted by CERT-In empaneled auditors, must also be submitted by the payment aggregator within two months of the close of the financial year to the RBI.
- Payment aggregators should have a Board approved information security policy and IT governance with a major involvement from the Board. An IT Steering Committee is to be created with representations from various business functions. An enterprise information model is also required to enable application development and decision-supporting activities, consistent with board approved IT strategy.
- Entities are also required to maintain an enterprise data dictionary incorporating the organisation's data syntax rules to enable sharing of data across applications and systems. The other requirements include, having a competent staff, undertaking vendor risk management, and a cryptographic requirement for encryption algorithms based on well-established international standards.
- The entities are also required to take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions and consider appropriate controls to prevent unauthorised access to the data.
- Apart from the above, the recommendations encapsulate a variety of requirements, such as having a comprehensive information security governance policy, risk assessment, data security standards, and best practices such as PCI-DSS, PA-DSS, latest encryption standards, and transport channel security.

The above measures are indicative of the RBI's focus on data protection and security that payment aggregators need to be mindful of when undertaking transactions.

Key considerations for payment aggregators

Apart from the abovementioned technology and security-related measures to be undertaken, payment aggregators also need to adhere to other conditions, including some of the key ones highlighted below:

- Choice of entity: Non-bank payment aggregators are required to be companies incorporated in India under the Companies Act, 2013 and their Memorandum of Association must cover the proposed activity of operating as a payment aggregator. An LLP, branch, or liaison office for instance, would not be eligible for such RBI authorisation.
- Marketplaces: E-commerce marketplaces also providing payment aggregator services will need to split the businesses and apply for authorisation as a payment aggregator on or before 30 June 2021.
- Settlement account: The notable features of the Guidelines include the requirement of an escrow account designated as the settlement account, which must be opened by the payment aggregator entity with a

scheduled commercial bank. This replaces the nodal account that intermediaries had to open with banks under the 2009 Directions. The importance of this settlement escrow account is that the amounts deducted from the consumer's account must flow through this settlement escrow account before being disbursed to merchants. There are clearly set out debits and credits permitted to be made from this settlement escrow account which cannot be deviated from when operating the account. The Guidelines also set out clear settlement timelines for payments flow which the payment aggregator must adhere to.

- Merchant onboarding: The payment aggregator is also required to conduct background and antecedent checks on the merchant to ensure that they do not have a history of duping customers or selling fake, counterfeit, or prohibited products.
- Governance: A payment aggregator is also required to have a board approved policy for the disposal of complaints or dispute resolution mechanism and timelines for processing refunds as per the timelines prescribed by the RBI. The Guidelines additionally stipulate the designation of a nodal officer who is to ensure compliance with regulatory functions and handle customer complaints along with escalation matrix.
- Know Your Customer ('KYC'): The Guidelines also make prevailing KYC norms applicable to payment aggregators. Though unclear, it appears that payment aggregators and gateways are required to conduct KYC checks on their customers, which may be merchants and/or end users, on the nature of each arrangement.

The way forward

The Guidelines are set to have a far-reaching impact on existing payment aggregators as well as new entrants into the market. Although payment aggregators are dependent on banks and card networks to facilitate and process transactions, payment aggregators are to be placed on the same pedestal as regulated payment system providers (such as e-wallet providers) under the Guidelines. Hence, the Guidelines do appear to be excessive in terms of the extent of regulation.

From a commercial standpoint, online businesses and payment aggregators would need to revisit their contractual arrangements and payment mechanics to transition to the new regime under the Guidelines. Furthermore, there are multiple obligations that appear onerous and an impediment to business operations. For instance, payment aggregators are tasked with carrying out background checks on the merchant's history to ensure that they do not have a stained history. This may be onerous and practically difficult to implement.

There are restrictions on merchants and payment aggregators storing customer card data, irrespective of the technology and data security related compliances undertaken. This would have a business and commercial impact on merchants that require customer payment information to provide a smooth user experience, for instance to initiate recurring payments towards subscriptions, refunds, service requests, billing, and transaction

records, and switching payment aggregators in case of service disruption. Restrictions on merchants and payment aggregators in storing such customer payment data on file would result in disrupted business operations and negatively impact the customer experience

In terms of data sovereignty, there is scope for such provision to be interpreted vaguely. Wholly owned subsidiary of a foreign company or any other Indian owned/controlled entity using foreign technology to provide data storage services to payment aggregators will need to evaluate whether they fulfil the necessary data compliance requirements.

The above issues are merely indicative that the Guidelines will have to slowly adapt to ensure a balance between ease of online business on one hand and safety and security of online transaction on the other. Some of the concerns and ambiguities is under consideration by the RBI basis industry feedback. We hope that they will be ironed out by the RBI by way of adequate FAQs/clarifications.

Sanjana Rao Member, Regulatory Practice Group
sanjana.rao@nishithdesai.com
Aaron Kamath Leader, FinTech Practice Group
aaron.kamath@nishithdesai.com
Vivek Kathpalia Head, Singapore Office
vivek.kathpalia@nishithdesai.com
Nishith Desai Associates, Bangalore, New Delhi, and Singapore

---

1. See: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
2. See: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11910&Mode=0
3. See: https://www.business-standard.com/article/finance/digital-transactions-could-reach-rs-15-trillion-a-day-by-2025-rbi-120072201431_1.html
4. See: https://www.rbi.org.in/Scripts/ATMView.aspx?atmid=113
5. See: https://www.rbi.org.in/Scripts/NEFTUserView.aspx?Id=147
6. See: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=5379&Mode=0
7. See: https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=943