NASSCOM®

NASSCOM's feedback to the Reserve Bank of India (RBI) on 'Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators' dated September 17, 2019

Feedback on RBI's 'Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators'

We thank the Reserve Bank of India (**RBI**) for this opportunity to present our views and suggestions on the *Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators* (**Discussion Paper**).[1] It presents a detailed assessment of the payments ecosystem in the country, covers the various facets of the activities of the Payment Gateways (**PG**) and Payment Aggregators (**PA**) and presents different options towards their regulation.

Based on inputs from our members and other stakeholders, we have prepared our response, which reviews the various aspects of the Discussion Paper along with our comments and suggestions.

Current Regulatory Position

The operations of PGs/ PAs are indirectly regulated by the RBI under the *Directions for opening and operation of accounts and settlement of payments for electronic payment transactions involving intermediaries* (**2009 Directions**).[2] PGs/PAs fall under the definition of **"intermediaries"** of the extant regulations. "*Intermediaries would include all entities that collect monies received from customers for payment to merchants using any electronic/online payment mode, for goods and services availed by them and subsequently facilitate the transfer of these monies to the merchants in final settlement of the obligations of the paying customers*."

In addition to the obligations under the 2009 directions, payment industry players, including PGs/PAs, also abide by existing card schemes rules, contractual agreements with banks, the Payment Card Industry Data Security Standard (**PCI-DSS**) and Payment Application Data Security Standard (**PA-DSS**), and other requisite compliances under the provisions of the Information Technology Act 2008 and the newly passed Consumer Protection Act 2019.

NASSCOM Recommendations

As the RBI has rightly acknowledged, the current framework of indirect regulation has ensured the absence of any major complaint in the last ten years, thereby testifying for the adequacy of the existing governance framework. We agree that the extant regulations are sufficient to address the concerns and gaps highlighted in the Discussion Paper, as they have been doing over the last decade.

Nonetheless, we welcome regulatory improvements. We recommend that the risks underlying the proposals be appropriately addressed with a light-touch regulatory framework akin to a hybrid of Options 1 and 2 as put forth in the discussion paper.

[1] Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators, September 17, 2019. See: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=943

[2] Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries, November 24, 2009. See: https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5379

Accordingly, we have reviewed the specific proposals under the proposed Option 3 ("**Full Regulation**") and have recommended what we consider to be suitable for a light touch and effective framework.

I. Scope of Discussion Paper

Based on our member consultations, we are of the view that the Discussion Paper should not limit its scope to PGs and PAs; instead, it should cover all the payment intermediaries who process payments instructions and have access to customer's payments data. Such intermediaries can be categorized as follows-

1. Banks acting as payment intermediaries
2. Non-banks payment intermediaries having nodal accounts with banks
3. Non-banks payment intermediaries operating without nodal accounts, but in partnership with banks
4. Third party apps/platforms (e.g. WhatsApp, G-Pay, etc.) that provide payment services using platforms (e.g. Unified Payments Interface (**UPI**), Immediate Payment Service (**IMPS**), etc.) operated by retail payment organisations (e.g. the National Payments Corporation of India (**NPCI**)) in partnership with banks.

We recommend RBI to use the above four categories for the purposes of the proposed framework.

All remaining intermediaries in the payment ecosystem, should be treated as pure technology service providers, and be excluded from the scope of this framework. Any risk associated with such pure technology service providers should continue to be addressed through contractual agreements with RBI regulated entities.

II. Risk Based Regulation

The primary objective of 2009 Directions was to safeguard the interests of the customers and to clarify the obligations of intermediaries receiving and processing payments from these customers from the online/ electronic payment modes. As the Discussion Paper has rightly observed in Paragraph 3.3, "*...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."*

We believe that the success of the extant framework is largely due to it being aligned closely and proportionately to the risks associated with payment intermediaries' activities.

Accordingly, the remainder of our recommendation, tries to evaluate the actual existence of various risks, and recommends proportionate and appropriate regulatory options.

1. Settlement Risk

a) Opt-in for Direct Regulation in Certain Cases

As mentioned, the 2009 Directions require all intermediaries to maintain a nodal account with a bank, which shall be an internal account of the bank, with permitted debits and credits. This arrangement has contained settlement and insolvency risks that could be associated with payment intermediaries. Even otherwise, in situations where payment intermediaries operate through other account arrangements (including an escrow account) settlement risks are sufficiently mitigated by ensuring that banks retain control over the settlement account, and that all payment instructions are netted out in the settlement account.

However, based on our member consultations, we note that some PGs/PAs might want to have greater control over the settlement account for the sole purpose of being able to provide better services to their merchants/ customer. For instance, if a PG is provided direct control of the settlement account, then they would not have to rely on their partner banks for reducing the settlement timelines for merchants and could accordingly provide faster and more frictionless payments for both merchants and consumers. However, in instances where a PG/PA is desirous of having greater control over the settlement account, appropriate regulatory obligations would be imposed directly upon such PG/PA, in order to mitigate settlement risks.

It is submitted, that only in such cases where certain PAs/PGs opt-in for direct regulation, should minimum capital requirements be considered by the RBI, since in its current form, we feel that the minimum capital requirement proposed by the RBI, is disproportionate to the risks associated with the activities of a majority of PAs/PGs.

To contextualize, the Securities and Exchange Board of India (**SEBI**), requires the maintenance of a minimum capital requirement of ₹50 by mutual funds within three years as part of its attempts to discourage 'non-serious' players from staying in the business.[3] This threshold was only ₹10 crore till 2014. Mutual funds and PAs/PGs both do not place consumers at a high risk on account of insolvency risks. However, both require a suitable fit and proper threshold for IT and fraud risk management. PAs/ PGs offer greater regulatory comfort as they are bound by contractual relations with RBI regulated entities. Therefore, the need for a high minimum capital requirement should be revisited.

A minimum capital requirement such as that proposed by the RBI under the discussion paper, would raise market entry barriers for new players and start-ups looking to enter the payments ecosystem, and provide new and innovative intermediary services. At the same time, such a requirement will result in concentration of this business on the hands of few players dominating the business.

Accordingly, we would urge the RBI to first consider qualitative capital or “fit and proper” requirements, and limit the actual specification of minimum capital

---

[3] Securities And Exchange Board Of India (Mutual Funds)(Amendment) Regulations, 2014, May 6, 2014. See: https://www.sebi.gov.in/sebi_data/commondocs/SEBIMFAMENDREGU-2-14_p.pdf

requirements to only such PAs/PGs who may want greater control over the settlement account.

Recommendation 1: *RBI may look at framing guidelines that provide for a tiered regulatory structure like a category 1 and category 2 Pas/ PGs. Certain additional benefits/ facilities may be provided to such intermediaries who seek greater access of the settlement account, and corresponding regulatory obligations. The RBI may issue a subsequent consultation detailing out specific obligations and benefits to be included in such a framework.*

The existing 2009 Directions and the manner in which PGs/ PAs operate today, ensures the safety and security of funds being transferred, and mitigates all associated settlement and insolvency risks. Accordingly, the RBI may broadly continue with the same arrangement for PAs/ PGs that continue to operate in the existing structure and do not involve any new risk.

Recommendation 2: *Only in cases where PAs/PGs opt-in for greater and direct regulation, in line with what has been indicated in Recommendation 1, should the RBI consider prescribing a risk appropriate capital requirement. Even in this scenario, the proposed minimum capital requirement is high and should be reviewed downwards.*

b) Nodal vs Escrow Account

The Discussion Paper states that if Option 3 is exercised, the basis of regulation according to Section 6.3 will be as follows-

"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."

The 2009 Directions, on the other hand, recognises the role of nodal account and expressly bestows the responsibility to maintain and operate such an account only with the bank. It expressly states that such accounts are not to be maintained or operated by the PGs/PAs. Such nodal accounts are subjected to audits by independent third parties, which provides another layer of protection to the funds in the nodal account.

Mandatory implementation of escrow account will affect the existing arrangements between the industry players; it may have a ripple effect on other entities in the payment system, and may disrupt the growth of the industry and the economy.

***Recommendation 3**: RBI should provide PGs/PAs the freedom to opt for settlement mechanisms. This could either be the existing arrangement of maintaining a nodal account. Alternately, a PG/PA could choose to maintain an escrow account with a bank for the purposes of settlement of merchant amounts. In such a scenario, the RBI could consider additional benefits and obligations for those that opt to operate via an escrow account. This will enable the payment intermediaries' greater flexibility in mitigating the settlement risk.*

c) Definition of "T"

The definition of 'T' under the 2009 Directions, ensure that customer money will be settled with the merchant only once the customer-initiated transaction has been completed. The manner in which a transaction can be considered to be 'completed' may vary depending on the product/ service or the business of the merchant and it is important to retain such flexibility to create a balance between customer and merchant rights.

At present, Option 1 in the Discussion Paper refers to making minor changes to the definition of 'T'. However, these changes have not been mentioned in the Discussion Paper.

Assuming, that the changes that the RBI wishes to propose under Option 1, are similar to the proposal presented in the Discussion Paper under Option 3 – there still remains a need for additional clarity on how the new definitions of T, T_S and T_D are to factor into the actual timelines for settlement of funds. This comes to be of particular importance, given significant variances in the business models adopted by merchants operating in India

***Recommendation 4:** RBI should retain the existing definition of 'T' as provided under the 2009 Directions. Should the RBI wish to modify this definition, then we request the RBI to clarify the changes it wishes to make to the applicable rules on settlement timeline, and place the same for industry consultations.*

d) Exemptions under Section 5.2 of the Discussion Paper

Section 5.2 of the Discussion Paper proposes certain exclusions from the scope of any eventual regulatory framework. We note that these exemptions include "e-commerce marketplaces".

At present, it is not clear whether this exemption has been made in light of the RBI's proposal to require e-commerce marketplaces to bifurcate their payments' business from that of their marketplace business. In case of an "e-commerce marketplace", services in the nature of PGs/ PAs sit adjacent to various services that the platform provides. As long as they comply with the applicable regulations, it is not clear why it should be necessary for them to separate the payment intermediary activities into a different legal entity.

Recommendation 5: *The RBI should continue to allow the e-commerce marketplaces to undertake activities as payment intermediaries and require them to comply with applicable regulations. The option of operating the PGs/PAs activities in a separate legal entity should be left to the e-commerce marketplaces.*

2. Data and IT Security Risk

a) Securing Customer Data

All PGs/ PAs handling customer card details are today required to be PCI-DSS complaint, in addition to complying with applicable obligations under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[4]

These rules will soon be superseded by an overarching Personal Data Protection law, which is already at advanced stages. Once enacted, this law would operate as an overarching regulation governing the collection, transfer, use, storage etc. of personal and sensitive personal data of customers, including payments data. Accordingly, all PGs/PAs and even merchants collecting and/or processing customer data would be regulated either as "data fiduciaries" or "data processors" under the law.

The above controls would significantly mitigate any risk to the customers'/ merchants' money and payment data being handled by all players in the payment ecosystem.

Recommendation 6: *The existing 2009 Directions and the manner in which PGs/ PAs operate today, ensures the safety and security of the money and payment data being processed through such payment entities therefore the additional measures proposed under section 6.6 of the Discussion Paper are not needed.*

Further, we recommend that the RBI take no further measures in this regard till the enactment of the Personal Data Protection law. Thereafter, assessing on its own account the effectiveness of the new framework, If the RBI still observes any additional risks to customer data, then it may consider additional regulations.

b) IT Systems Security

Apart from the adoption of existing data security standards under PCI-DSS, PAs/PGs are also held accountable from an IT systems risk perspective, through contractual arrangements entered into between banks and PAs/PGs. These include obligations for breach and security incident reporting, and fixation of liability in the event of a security incident.

Likewise, UPI based PSPs are also complying with relevant IT security risk mitigation obligations imposed by way of the NPCI's UPI Procedural Guidelines, which require all UPI applications to be pre-certified by the NPCI, and abide by relevant requirements for secure customer registration and transaction layer security.

[4] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, April 11, 2011. See: https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

Recommendation 7:

The RBI may consider a requirement of annual security and process audits through CERT-IN empaneled independent auditors, in addition to the existing indirect regulatory framework. The RBI should broadly continue with the current approach, where a combination of contractual obligations and self-regulation, have ensured that no major security incidents have threatened the integrity of payment systems.

3. Grievance Redressal

Under Option 3 of the Discussion Paper, a *Customer Grievance Redressal and Dispute Management Framework* has been proposed, which includes designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution.

We note that the Ombudsman Scheme for Digital Transactions, 2019 (**2019 Ombudsman Scheme**), which came into force earlier this year, already provides an additional layer of protection and recourse for aggrieved customers.[5]

We believe that the current internal measures put in place by PAs/PGs for customer grievance redressal, together with the 2019 Ombudsman Scheme are sufficient to address most customer complaints/grievances.

Nonetheless, should the RBI want a more prescriptive mechanism for customer grievance redressal by PAs/PGs, then it may consider introducing such a framework only for certain large PAs/PGs based on a threshold of transactions processed by value. If based on its observation of this experience, the RBI is satisfied with the framework's efficacy, it may consider extending this framework to other firms, going forward.

Recommendation 8: Dispute resolution mechanisms maintained by PAs/PGs internally, together with the 2019 Ombudsman Scheme, address all customer grievances/disputes, as on date.

Nonetheless, if the RBI be desirous of strengthening the framework for customer grievance redressal, it should test the applicability of such a framework to only such PAs/PGs that go over a certain transaction value threshold. It may even invite PAs/PGs to opt in to such a framework. This should offer an opportunity to the PAs/PGs to differentiate themselves and allow the RBI to assess the efficacy of the measure before deciding if it would be useful to mandate it.

4. Systemic Risk

Risks arising out of the activities of PAs/PGs that could have systemic ramifications are typically limited to Anti-Money Laundering (**AML**) risks, insolvency risks and IT security risks. As discussed under Recommendation 12 below, AML risks are adequately mitigated through existing Know-your-Customer (**KYC**) compliances made applicable to regulated entities.

[5] Ombudsman Scheme for Digital Transactions, January 31, 2019. See: https://cms.rbi.org.in/cms/Documents/en-US/Ombudsman%20Scheme%20for%20Digital%20Transactions%202019.pdf

Likewise, insolvency risks are also adequately mitigated through the current framework of indirect regulation, since insolvency of a PA/PG will not impact customer and merchant funds, which are to be held and settled through nodal accounts classified as internal accounts of banks, or as escrow accounts. Further with the passage of the Insolvency and Bankruptcy Code, 2016 (**IBC**) the requirement for the Insolvency Professional to ensure the resolution of a company's insolvency as that of a going-concern further mitigate insolvency risks, since all unsettled merchant dues will have to be settled first as an operational debt.

Likewise, in addition to existing self-regulatory standards such as PCI-DSS and PA-DSS, IT and data security risks will be further mitigated for all players in the payments ecosystem with the enactment of the Personal Data Protection Law (*See* Recommendations 6 and 7).

However, none of the existing PAs/PGs are at such a scale as to pose systemic risks upon the existing payments infrastructure, and the financial system at large. The retail payment ecosystem has expanded significantly in recent years, and no single mode of retail payments, e.g. card networks, wallets, bank-based payment networks, services offered by retail payment organisations such as NPCI. Resultantly, in the context of the risks highlighted above (AML, IT security and insolvency risks), the non-availability of even a significant PA/PG, would not lead to systemic consequences.

In fact, to the best of our knowledge, no other jurisdiction currently regulates any PA/PG as a Systematically Important Payment System (**SIPS**). Accordingly, and in the absence of systemic risks associated with PAs/PGs, there isn't a strong enough case for direct regulation of PAs/PGs by the RBI.

Recommendation 9: RBI as the supervisory institution for the banking and financial system should ideally limit its direct regulatory oversight to such payment systems that could pose a systemic risk. Accordingly, we urge the RBI to continue with the existing indirect regulatory approach.

5. Other salient points for RBI consideration and feedback

(i) Segregation between e-commerce marketplace entity and PGs/PAs

This provision requires clear distinction between e-commerce marketplace entity and PGs/PAs and mandates operating the payment gateway services business under a separate entity. The Discussion Paper also provides a timeline of 3 months for existing e-commerce marketplaces acting as PG/PA to other merchants to segregate the business.

Recommendation 10: As stated in recommendation 5, it is not recommended to mandate the e-commerce marketplace entities to operate PGs/ PAs under a separate entity. However, if the RBI decides to go ahead with this, it should consider allow a period of 6 months, instead of the proposed 3 months, to existing e-commerce marketplaces acting as PG/PA to other merchants to segregate the business.

(ii) Merchant Presence in India

According to Section 1.8 of the Discussion Paper, "*Payment Gateways and Payment Aggregators shall deal with only those merchants who have a physical presence in the country.*" This provision restricts PAs/PGs to deal with only merchants who have a presence in India. It is submitted that there are existing regulations under the Foreign Exchange Management Ac, 1999 (**FEMA**), the RBI Circular on Processing and Settlement of Import and Export related payments facilitated by Online Payment Gateway Service Providers dated 24 September 2014 (**OPGSP Circular**) and the Security Issues and Risk Mitigation measures related to Card Not Present (**CNP**) transactions dated 22 August 2015 that regulate the role of a PG/PA in relation to transactions to be made to offshore merchants. Therefore, instead of prohibiting PGs and PAs from dealing with merchants who do not have a physical presence in the country, the regulation can stipulate that PGs/PAs may follow all existing regulations and circulars issued by the RBI while dealing with offshore merchants.

Recommendation 11: RBI should consider dropping the requirement for local incorporation of merchants, and instead ensure that PGs/PAs are in compliance with existing regulations in this regard. Further, since PGs/PAs use Category 1 AD bankers for making payments outside India, all the documentation requirements for making remittances can be done by PGs/PAs on behalf of the customers.

(iii) Merchant KYC

RBI has recommended that PGs/ PAs must undertake KYC of the merchants prior to on-boarding such merchants. In respect of KYC compliance, banks and financial institutions are already required to undertake KYC checks of merchants and therefore imposition of an additional layer of merchant KYC by PGs/ PAs will be a mere duplication of an activity that is already undertaken by regulated entities such as banks. Further, imposition of KYC directions on PGs/ PAs will also impose additional costs on the technological structure incorporated by intermediaries since their infrastructure currently does not support KYC checks; thereby increasing merchant on-boarding and overall transaction costs. Customers would also be inconvenienced if such added obligations are notified in the present form. KYC obligations on PGs/ PAs has the potential to threaten the growth of digital payment systems in the country on account of such costs being commercially unviable.

Recommendation 12: In order to address any concerns of RBI, the PA/PG can be required to collect name, address, PAN and GST (wherever applicable) only when on-boarding is via digital means. Other than that, an added KYC check by PGs/ PAs is not required given that merchants that are on-boarded by PGs/ PAs are already required to be KYC compliant. To that extent, all payment transactions with merchants operate in a KYC compliant ecosystem, with the issuing and acquiring banks having already undertaken KYC verification of both their customers and merchants.
