Comments to the Reserve Bank of India (RBI) on the Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators (the Discussion Paper) dated 17 September 2019

Dvara Research[1] is an Indian not-for-profit policy research and advocacy institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. Our work addresses emerging issues in policy and regulation for consumer protection, given the sweeping changes that are reshaping retail financial services in India. The effects of disintermediation in finance, including through the growth of fintech, is a core area of our recent research.

In this Response, we present our comments on the RBI's Discussion Paper on the Guidelines for Payment Gateways (PG) and Payment Aggregators (PA) in response to the call for comments from stakeholders (Reserve Bank of India, 2019c). Our comments are organised into five broad themes, which will seek to convey and substantiate the following feedback to the Discussion Paper.

1. Clearer articulation of regulatory objectives is required to assess the proportionality of proposed regulation and to prevent duplication of regulatory efforts.
2. Clarity is sought on the rationale guiding the distinction between payments gateways and payments aggregators.
3. More detail on Option 1 and Option 2 of the proposed policy alternatives would enable a better comparison of their relative costs and benefits.
4. The need to harmonise the proposed consumer grievance redress framework with existing consumer recourse mechanisms.
5. We welcome the extension of IT security standards and urge for symmetric regulation of all digital financial activities to ensure uniform treatment of users' data.

This Response seeks to provide constructive comments on the Discussion Paper. We hope they will be considered and addressed in future iterations of the Guidelines for Payment Gateways and Payment Aggregators.

[1] Dvara Research (formerly the IFMR Finance Foundation) has made several contributions to the Indian financial system and participated in engagements with key regulators and the Government of India. We were the technical secretariat to the RBI's Committee on Comprehensive Financial Services for Small Businesses and Low Income Households chaired by Dr Nachiket Mor. We acted as peer reviewers for the customer protection recommendations made by the Financial Sector Legislative Reforms Committee. Our recent research has given us the opportunity to consult on and extend discrete research inputs to various Committees set up by the RBI and the Government of India, including the Committee of Experts (on data protection) under the Chairmanship of Justice B.N. Srikrishna, RBI's Committee of Fintech & Digital Banking, the RBI's Expert Committee on Micro, Small & Medium Enterprises and the RBI's Committee on Deepening of Digital Payments.

1. **Clearer articulation of regulatory objectives is required to assess the proportionality of proposed regulation and to prevent duplication of regulatory efforts.**

Regulations are often designed to remedy market failures (Government of India, 2013). Objectives of financial regulations include (1) sustaining systemic stability, (2) maintaining the safety and soundness of financial institutions, and (3) protecting the consumer (Llewellyn, 1995). The Discussion Paper in Section 3 impresses upon the growing significance of Payments Gateways (PGs) and Payments Aggregators (PAs) and set out gaps and concerns in the existing regulation. However, it falls short of articulating the market failure or the specific objective of financial regulation that motivates this regulatory intervention. This lack of clarity on policy objectives creates at least two analytical problems:

i. *Makes it difficult to assess the proportionality of the proposed policy objectives:* In the absence of well-defined regulatory challenges, policy objectives, or risks being addressed, it is difficult to adjudge if the proposed policy alternatives are proportionate and effective. For instance, it is hard to ascertain if PAs or PGs merit maintaining a net-worth of INR 100 crores, as proposed in the third policy alternative set out in section 4.3.2(ii) of the Discussion Paper. Without sufficient discussion on the financial risks and financial stability concerns being addressed through these capital requirements, these regulatory requirements appear onerous. Prepaid Payment Instruments (PPIs), which generate similar risks, have a net-worth requirement of INR 15 crores (Reserve Bank of India, 2019b). The proposed net-worth requirements of the PAs and PGs resemble those of Small Finance Banks (SFB), despite SFBs facing credit, market and operational risks (Reserve Bank of India, 2014). A clear articulation of the financial and consumer protection risks and the financial stability risks that are being addressed is needed to assess the effectiveness and proportionality of the proposed regulatory alternatives.

ii. *Duplication of regulatory efforts:* The lack of clear objectives can also lead to the duplication of regulatory efforts of other regulators. For instance, the Discussion Paper in section 6.1 suggests that PAs & PGs must *"undertake background checks to ensure that merchants do not have an intention to defraud customers or sell fake, counterfeit or prohibited goods."* Section 6.2 further urges PAs and PGs to *"check the merchant's website for authenticity and security purposes."* These concerns around the quality of goods and the authenticity of the retailer resemble the mandate of the consumer protection framework. The Consumer Protection Act (Ministry of Consumer Affairs, Food & Public Distribution,

2019) and the apparatus under it, is created exclusively to protect consumers' interest and offer timely settlements of consumers' disputes. The effectiveness of mandating PGs and PAs to perform this function appears questionable. A similar duplication of this mandate also appears in section 6.3 of the Discussion Paper which requires PAs and PGs to *"consider information disclosure policies, privacy policies and digital footprints while conducting due diligence."* PAs and PGs may not be well equipped to analyse merchants' privacy policies which appear to be the domain of skilled "data auditors" being considered in the Draft Data Personal Protection Bill (The Draft Personal Data Protection Bill, 2018).

2. We seek clarity on the rationale guiding the distinction between payments gateways and payments aggregators.

The Glossary of the Discussion Paper defines PA as "*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"*. A PG is defined as *"a technology infrastructure provider to route and facilitate processing of an online payment transaction, without any involvement in the actual handling of funds"*.

The distinction between PAs and PGs appears to turn on the management of funds. However, it is understood that PAs facilitate payments through a nodal account that are the internal accounts of the relevant sponsor bank, and sit on the bank's balance sheet. This is reflected in the RBI's 2009 Directions for opening and operation of accounts and settlement of payments for electronic payment transactions involving intermediaries (Reserve Bank of India, 2009).

As background, in 2009, upon witnessing the surge in the use of electronic and online payment modes for bill payments, online shopping etc., the RBI had issued directions for settlement of payments for electronic payment transactions that involved intermediaries such as payment aggregators and payment gateways. These were issued with the view of safeguarding the interests of consumers (Reserve Bank of India, 2009). In accordance with these directions, the nodal accounts opened and maintained for facilitating collection of payments by intermediaries from customers of merchants, shall be treated as internal accounts of the banks and will not be operated by the intermediaries. Given the reality of existing arrangements (and nodal account ownership), the definition of the PAs in the Discussion Paper appears to merit deeper consideration.

Seminal scholarship on regulation establishes the relative superiority of regulating financial activities as opposed to institutions performing the activity (Merton, 1995). If a distinction is being made between PAs and PGs, the risks this distinction is seeking to address at a functional level must be made clear. While regulations regarding IT security, consumer protection, contractual clarity etc. maybe welcome for PAs, it is unclear that the distinction based on the factors reflected in the current definition is appropriate.

3. More detail on Option 1 and Option 2 of the proposed policy alternatives would enable a better comparison of their relative costs and benefits.

The Discussion Paper in Section 4 set out three mutually exclusive policy options for regulating PAs and PGs. We commend the detailed elaboration of Option 3 (Full and Direct Regulation) in the Discussion Paper. However, in the absence of similar detailed description of the other two options, it is hard to assess the relative merit of each policy alternative.

Option 1 (Continue with the extant instructions) entails continuing with the current regulatory framework applicable to PAs and PGs. Option 2 (Limited Regulation) set out in section 4.2 seeks to furnish regulatory requirements for PAs and PGs with respect to *"minimum net-worth, merchant on-boarding, timelines for settlement of funds, maintenance of escrow account, IT security, etc."*, and subjecting them to reporting requirements of the RBI. However, there is no further explanation of what these regulations would entail and the obligations they would impose on PAs and PGs. The third regulatory alternative is presented in Option 3 (Full and Direct Regulation). It lays out the conditions for licensing and authorisation, corporate governance, grievance redress and discusses each insignificant detail.

The selection of appropriate regulatory stance often involves assessing relative advantages of different policy alternatives along with multi-dimensional criteria such as legal feasibility, economic viability, effectiveness and efficiency and coherence with other policy objectives (How to Identify policy options, Better Regulation Toolbox). The lack of detail on competing policy alternatives (Options 1 and 2) prevents an in-depth analysis of the relative merits and demerits of policy alternatives. In the absence of a comprehensive understanding of the relative costs and benefits of policy alternatives, it is hard to recommend a policy alternative with certainty.

4. The proposed consumer grievance redress framework needs to be harmonised with existing consumer recourse mechanisms.

We welcome the effort of the regulator to create a robust grievance redress and recourse mechanism for consumers of PAs and PGs. The Discussion Paper in section 3.2 emphasises limited access that consumers may have to PAs and PGs in the event of a grievance.

We note that the proposed grievance redress mechanism is distinct from but closely resembles the existing Ombudsman Scheme for Digital Transactions (OSDT) (Reserve Bank of India, 2019a). This regulatory choice of setting a distinct redress framework for PGs and PAs appears to be divergent from the RBI's previously documented regulatory preference of bringing PAs under the ambit of the OSDT. In the Benchmarking India's Payment Systems Report published earlier in June 2019 the RBI cited the need to regulate PAs to bring them in the regulatory perimeter of the OSDT (Department of Payment and Settlement Systems, 2019a). The rationale of duplicating another recourse mechanism instead of expanding the jurisdiction of the existing OSDT remains unclear.

The duplication of a recourse mechanism also deviates from the government's long-standing and well-reasoned recommendation of creating a unified financial redress agency for consumers. The Task Force on Financial Redress Agency (Government of India, June 2016) found that the existing grievance redress mechanisms in finance were highly fragmented, non-uniform and proved to be onerous for the consumers. India's existing financial redress mechanism exerts consumers by making them *"approach different channels for redress, based on whether their complaint falls under banking; insurance; pension; securities market or other financial services* (Government of India, June 2016)*."* It renders grievance redress expensive, inaccessible and ineffective for consumers constrained for time, money and agency. In this context, creating two parallel channels for registering complaints related to digital transactions will exert consumers even further. It is especially true of consumers who are first-generation users of digital finance in India. Our findings from the field suggest that users find themselves ill-equipped to seek redress, especially in the digital economy due to lack of digital literacy and familiarity with the digital economy (Dvara, CGAP, & Dalberg, 2017). Considering the users' lack of familiarity with the digital ecosystem, weighing them down with multiple, fragmented and siloed recourse mechanisms will disempower them further. It is also worth reiterating that multiple, parallel and fragmented channels of recourse also increase the chances of gaps in

regulation and regulatory arbitrage (Government of India, June 2016), potentially offering little recourse to the consumer.

5. We welcome the extension of IT security standards and urge for symmetric regulation of all digital financial activities to ensure uniform treatment of users' data.

The Discussion Paper stipulates a *Security, Fraud Prevention and Risk Management Framework* for PGs and PAs in Annex 2 if the third option of Full and Direct Regulation is exercised.

The Payments and Settlements Systems Act 2007, empowers the RBI to issue regulations indicating the standards of security for information technology infrastructure. Consequently, the RBI regularly issues guidelines on IT security standards and cybersecurity of entities under the PSSA. For instance, prepaid payment instruments (PPI) witnessed a rise in their uptake towards the end of 2016. At the time the RBI issued a notification to system providers and system participants using section 10(2)[2] and section 18[3] of the PSS Act. It advised them to undertake cybersecurity audits with CERT-In empanelled auditors and comply with best practices for system infrastructure security (Reserve Bank of India, 2016b). The RBI has also recommended detailed cybersecurity frameworks for scheduled commercial banks (SCBs) (Reserve Bank of India, 2016a) and urban cooperative banks (UCBs) (Reserve Bank of India, 2018).

Considering the increasingly significant role that PGs and PAs play in digital payments, a considered revaluation of their cybersecurity framework is welcome. Substantially, the security and risk management framework provided in this Discussion Paper appears to be similar to the *Cyber Security and Resilience Requirements* given in Annex 1 of the notification on *Cyber Security Framework in Banks.* According to this framework, the PGs and PAs are required to

[2] Section 10 of the PSS Act, 2007 (Power to determine standards): Section 10(2) states, "w*ithout prejudice to the provisions of sub-section (1), the Reserve Bank may, from time to time, issue such guidelines, as it may consider necessary for the proper and efficient management of the payment systems generally or with reference to any particular payment system*" (Reserve Bank of India, 2007).

[3] Section 18 of the PSS Act, 2007 (Power of Reserve Bank to give directions generally): Section 18 states, "w*ithout prejudice to the provisions of the foregoing, the Reserve Bank may, if it is satisfied that for the purpose of enabling it to regulate the payment systems or in the interest of management or operation of any of the payment systems or in public interest, it is necessary so to do, lay down policies relating to the regulation of payment systems including electronic, non-electronic, domestic and international payment systems affecting domestic transactions and give such directions in writing as it may consider necessary to system providers or the system participants or any other person either generally or to any such agency and in particular, pertaining to the conduct of business relating to payment systems*" (Reserve Bank of India, 2007).

put in place an Information Security policy for the safety and security of the payment systems operated by them that is approved by an internal board. All cybersecurity incidents and breaches are required to be reported to the Department of Payments and Settlements Systems (DPSS), the RBI and the Indian Computer Emergency Response Team (CERT-In) (Department of Payment and Settlement Systems, 2019). The indicative framework resembles the cybersecurity framework of other financial sector entities and is coherent with the reporting guidelines and auditing mechanisms of the Cyber Crisis Management Plan of CERT-In. Therefore, this appears to harmonise the cybersecurity requirements across financial sector, minimising the scope of regulatory arbitrage.

References

Reserve Bank of India. (2018, October 19). Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs). Mumbai. Retrieved from https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11397&Mode=0

(MeitY) Ministry of Electronics and Information Technology. (2018, July 27). *The Draft Personal Data Protection Bill*. Retrieved from Ministry of Electronics and Information Technology: https://meity.gov.in/content/personal-data-protection-bill-2018

Department of Payment and Settlement Systems. (2019a, June). *Benchmarking India's Payment Systems*. Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/BIPS04062019CE3C72E9873244ED8BAAE9C8FC5955A8.PDF

Department of Payment and Settlement Systems. (2019b, September). *Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators.* Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DPSSDISCUSSIONPAPEREFCF5B7E17F9431185BD4FD57E540F47.PDF

Dvara, CGAP, & Dalberg. (2017). *Privacy on the Line.* Dvara Research. Retrieved from https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

European Union. (n.d.). How to Identify policy options, Better Regulation Toolbox. Brussels. Retrieved October 17, 2019, from https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-17_en_0.pdf

Government of India. (2013, March). *Chapter 2: The tasks of financial law, Report of the Financial Sector Legislative Reforms Commission*. Retrieved from Department of Economic Affairs: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Government of India. (2013, March). *Chapter 3: Structure fo the regulator, Report of the Financial Sector Legislative Reforms Commission*. Retrieved from Department of Economic Affairs: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Government of India. (June 2016). *Report of the Task Force on Financial Redress Agency.*

Indian Computer Emergency Response Team. (2014, January 16). *Information Technology (The Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013*. Retrieved from Indian Computer Emergency Response Team (CERT-In): https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf

Indian Computer Emergency Response Team. (2018, January 13). *Cyber Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism.* Retrieved from Indian Computer Emergency Response Team (CERT-In): https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2018-0113.pdf

Merton, R. C. (1995). Functional perspective of financial intermediation. *Financial Management*. Retrieved from http://www.people.hbs.edu/rmerton/afunctionalperspective.pdf

Ministry of Consumer Affairs, Food & Public Distribution. (2019, August 9). *The Consumer Protection Act, 2019*. Retrieved from Department of Consumer Affairs: https://consumeraffairs.nic.in/sites/default/files/CP%20Act%202019.pdf

Ministry of Information Technology and Electronics. (n.a.). *Digital Payments Division*. Retrieved from Ministry of Information Technology and Electronics (MeitY): https://www.meity.gov.in/digidhan

RBI. (2019a). *RBI releases draft "Enabling Framework for Regulatory Sandbox".* Mumbai: Reserve Bank of India.

Reserve Bank of India. (2007, December 20). *Payment and Settlement Systems Act, 2007*. Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf

Reserve Bank of India. (2009, November 24). *Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries*. Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/DOIPS241109.pdf

Reserve Bank of India. (2014, November 27). *RBI releases Guidelines for Licensing of Small Finance Banks in the Private Sector*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=32614

Reserve Bank of India. (2016a, June 2). *Cyber Security Framework in Banks.* Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

Reserve Bank of India. (2016b, December 09). *Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=10772&fn=9&Mode=0

Reserve Bank of India. (2019a, January 31). *Ombudsman Scheme for Digital Transactions, 2019*. Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/Content/PDFs/OSDT31012019.pdf

Reserve Bank of India. (2019b, August 30). *Master Direction on Issuance and Operation of Prepaid Payment Instruments*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142

Reserve Bank of India. (2019c, September 17). *Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators*. Retrieved from Press Releases: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48173