

**Comments dated 14 April 2017 on the draft circular on “Master Directions on Issuance and Operation of Pre-paid Payment Instruments (PPIs) in India” (Draft Circular) released by the Reserve Bank of India (RBI)**

The Future of Finance Initiative (**FFI**) is housed within the IFMR Finance Foundation (**IFF**)<sup>1</sup> and aims to promote policy and regulatory strategies that protect individuals accessing finance given the sweeping changes that are reshaping retail financial services in India. Our vision is for every individual to have universal access to suitable financial services using a range of channels that enable them to transact securely and confidently.

We have listed our item-wise comments in the table below, referenced against the corresponding paragraph(s) of the Draft Circular.

<b>Sl. No.</b>	<b>Reference</b>	<b>Comment</b>
1.	4.2	<p>Further clarification is needed as to what the practice of ‘pre-funding’ is.</p> <p>In our view, as pre-funding is referred to in the context of cross border remittances for Bank issued PPIs, ‘pre-funding’ is the practice of 24-hour funding of merchant’s accounts in the debit cards market. The pre-funding amount is calculated based on the file of transactions submitted by the merchant to the debit card processor, without any review of the submitted transactions. If any cancelled or disputed transaction adjustments come in later upon review of a merchant’s transactions, the adjustments are sent through the following day to be deducted from the “pre-funded” account.</p>
2.	6.4	<p>The Draft Circular states that when an in-principle approval has been issued to a PPI issuing entity, that entity will need to submit System Audit Reports. However, it needs to be clarified as to which System Audit Report an entity with the in-principle approval needs to submit.</p>
3.	6.5	<p>The Draft Circular states that subsequent to the issuance of an in-principle approval, if any adverse features regarding the PPI issuing entity come to the fore then the approval will be withdrawn. We recommend that any such cancellation of in-principle approval be preceded by giving an opportunity to the concerned entity to present its case.</p>

<sup>1</sup> IFF is a policy research and advocacy institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. IFF has made several contributions to the Indian financial system and participated in engagements with all key financial sector 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’ (**CCFS**) (Chair: Dr. Nachiket Mor).

4.	6.8	The Draft Circular requires that any ‘material changes’ in the processes introduced by the PPI issuer will need prior approval of the RBI. However, further clarifications are needed regarding what constitutes ‘material changes’.
5.	6.10	While the provision to seek prior permission of the RBI for any changes in management or ownership is a positive development overall, (6.10 b) it is needlessly stringent as often times the number of directors in non-bank issuing companies is very low. Thus even in normal course of business, there is a high likelihood this trigger would get breached if 1-2 directors retire or get replaced for non-business reasons.
6.	8.8	Further clarification is needed regarding how PPI issuers will ensure that PPIs in their system are not created solely for facilitating cash-based remittances to bank accounts. Previous PPI circulars issued by the RBI have not carried this requirement and we were unsure of the need to have this now, given that cash loading in PPIs is proposed to be limited to Rs. 50,000 per month and all PPI users need to have full KYC in place.
7.	8.12(e)	<p>We note that in the context of digital financial services, customer data is being generated, collected, stored, processed and used at unprecedented rates and entire business sectors are being reshaped by building on data analytics.</p> <p>The current data protection regime in India contained in the Information Technology Act, 2000 framework mandates higher standards of care only for a narrowly defined set of ‘sensitive personal data or information’ (see Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011). In this context, we make a case for considering confidentiality of all “non-public personal information” (NPI) held by a PPI issuer in respect of a customer. The NPI may be disclosed by the PPI only with the prior written consent of the customer.</p> <p>It is relevant to note that the U.S. Gramm-Leach-Bliley Act, 1999 (GLBA, 1999) defines NPI as any “<i>personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.</i>” Examples of NPI include information obtained through Internet collection devices (i.e., cookies), list of a retailer's credit card customers and credit profiles of customers. The absence of protection for NPI has emerged as a significant risk in the context of digital financial services given that customer data is being generated, collected, stored, processed and used at unprecedented rates and entire business sectors are being reshaped by building on data analytics, and this needs to be urgently addressed.</p>

8.	9.3(a)	The requirement for all minimum detail semi-closed PPIs to be converted into full KYC semi-closed PPIs within a period of 60 days (assuming that the Draft Circular is notified on 1 May 2017) - failing which no further credit will be allowed into such PPIs - may be revisited in favour of logistical and operational ease. PPI issuers such as PayTM (One97 Communications Limited) claim to have crossed 200 million registered users and verification of the same may require a longer timeframe (Business Standard, 2017).
9.	11.2, 11.4	For bank issued PPIs, the outstanding balance is a part of the ‘net demand and time liabilities’, this enables banks to earn interest on the whole outstanding balance in their PPIs. However, non-bank issued PPIs can earn interest only on a “core portion” of their outstanding balances and that too only after a year of operations. Thus the Draft Master Circular creates an ecosystem where banks issuing PPIs can earn more income than non-banks issuing PPIs. We recommend that there be level playing field between bank and non-bank PPI players by providing that amounts collected by bank PPIs also be placed in escrow (which could be with a separate bank).
10.	15	We make a positive note that the security, fraud prevention and risk management framework under the Draft Circular corresponds closely with the RBI directions on cyber security in banks (RBI, 2016a). However, we also note that Information Technology (Security of Prepaid Payment Instruments) Rules 2017 – Draft ( <b>Draft Rules</b> ) (MeitY, 2017) issued by Ministry of Electronics and Information Technology, Government of India ( <b>MeitY</b> ) also propose to prescribe security standards for electronic PPI ( <b>e-PPI</b> ) issuers, which may result in overlapping or even conflicting compliances for such PPI issuers.
11.	16.2	<p>Grievance redressal is an important aspect of customer protection, the Draft Circular provides that:</p> <ul style="list-style-type: none"> <li>• non-bank PPI issuers should put in place and publicise an effective mechanism for redressal of customer complaints along with escalation matrix. Such issuers also have to report (i) customer complaints in the prescribed manner and frequency, and (ii) any frauds involving the instruments issued by them on a quarterly basis (or earlier),</li> <li>• customers of bank PPI issuers can approach the banking ombudsman for grievance redressal, and</li> <li>• banks shall also be responsible for addressing customer grievance issues for co-branded PPIs issued by them.</li> </ul>

		<p>By setting up parallel and different requirements, the Draft Circular can create confusion for the regulated entities. It could confuse customers to the extent that dual routes to complaints resolution are put in place by PPI issuers seeking to comply with RBI's mandate.</p> <p>Also, this provision takes away the ability of customers of non- bank PPI issuers to avail the banking ombudsman scheme of the RBI.</p> <p>In light of this, we recommend that the Draft Circular be amended to include non-bank PPIs under the banking ombudsman scheme for grievance redressal, till such time the Financial Redress Agency as envisaged by the Ministry of Finance, Government of India gets created.</p>
12.	16.5	<p>We recommend that customer liability for unauthorized / fraudulent transactions involving PPIs be clearly laid down in the Draft Circular on the lines of the Draft Circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions issued by the RBI on 11 August 2016 (RBI, 2016b). The referenced circular specifies conditions of zero customer liability as well as liability of customers being limited to transaction value or Rs. 5,000 (whichever is lower) along with timelines and related aspects.</p>
13.	18	<p>The proposal in paragraph 18 towards making compliant non-bank PPI issuers interoperable with payments systems is a positive move which will help increase the competition in the mobile payments market.</p>
14.		<p>There are several measures in the Draft Circular which overlap and conflict with the Draft Rules. While both set of measures often complement each other, the enactment of both set of measures could raise issues of dual regulations, conflicting requirements and adversely impact the ease of doing business. Please see the Annexure below for the details of these overlaps and conflicts.</p>

**ANNEXURE (ASSESSMENT OF THE DRAFT CIRCULAR AND THE DRAFT RULES)**

Sl. No.	Topic	Draft Circular Reference	Draft Rules Reference	Comments
1.	Definition of PPI versus e-PPI	2.1, 2.3	2(h), 2(n)	While the Draft Circular applies to all PPI issuers, the Draft Rules apply solely to e-PPI issuers. e-PPI issuers as defined by the Draft Rules are a subset of the PPI issuers as defined by the Draft Circular.
2.	Security standards	15.2	3,17(1), 17(2)	While both set of guidelines require the PPI issuers to develop and set an information security policy, the Draft Rules stipulate that MeitY may propose further security standards in the future for PPI issuers to abide by.
3.	Risk assessment policy	15.2, 17.1, 17.2, 17.3, 17.4 and 17.5	5(1), 5(2), 5(3)	Although the risk policy assessments of the Draft Circular and the Draft Rules largely overlap, the Draft Circular goes a step further and specifies in detail the procedural requirements of the system audit that has to be conducted by PPI issuers.
4.	Reporting of cyber security incidents	15.7	14(1), 14(2) and 14(3)	While both set of guidelines require PPI issuers to setup mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches, the Draft Rules go a step further and give specific guidelines to Indian Computer Emergency Response Team (CERT-In) for handling any incidents reported to it (paragraphs 14(2), 14(3)).
5.	Transaction authorisation	15.3(f)	6(3) and 6(4)	Both set of rules require Issuers to introduce multiple factor authentications for user transactions. But the Draft Rules in paragraph 6(4) state that the government may exempt PPI issuers from multiple factor authentication requirement in specified cases - depending on the amount, nature of transaction, risk involved and like factors. However, given the RBI's prior exemptions for small value card not present transaction from additional factor authentication (RBI, 2015), any Central Government exemption in the future may create conflict with the RBI regulations.

6.	Mechanisms for the procedure of authentication for accessing PPI accounts and fraud prevention	15.3(b), (c),(d), (e), (g), (h), (i), (j) and (k)	6(5)(a), (c), (d) and (e)	<ul style="list-style-type: none"> <li>• There is overlap, between 15.3(b) in the Draft Circular and 6.5(b) and (c) in the Draft Rules: while both set of measures require Issuers to place ‘appropriate mechanisms’ to restrict multiple invalid attempts to login/access to the PPI account - inactivity timeout features etc., the Draft Rules state specifically what the appropriate mechanisms should be.</li> <li>• There is also overlap between 15.3(i), (j) and (k) in the Draft Circular and 6(5)(e) in the Draft Rules: while both set of measures require Issuers to prevent, detect and block fraudulent payments before the e-PPI issuer’s final authorisation, the RBI rules specify what measures Issuers need to put in place to prevent fraud.</li> <li>• Other measures stipulated in 15.3 in Draft Circular complement paragraph 6(5) in the Draft Rules and set a higher set of security standards for PPIs.</li> </ul>
7.	Grievance redressal timelines	16.2(e)	16(3)	While Draft Circular gives PPI Issuers 48 hours to resolve a complaint, the Draft Rules give issuers 36 hours for the same.

## BIBLIOGRAPHY

- Business Standard (2017) Paytm crosses 200 million wallet user base [Online] Available at: [http://www.business-standard.com/article/companies/paytm-crosses-200-million-wallet-user-base-117022700773\\_1.html](http://www.business-standard.com/article/companies/paytm-crosses-200-million-wallet-user-base-117022700773_1.html) [Accessed 10 April 2017].
- Ministry of Electronics and Information Technology (2017) Information Technology (Security of Prepaid Payment Instruments) Rules 2017 – Draft, March 10, 2017 [Online] Available at: [http://meity.gov.in/sites/upload\\_files/dit/files/draft-rules-security%20of%20PPI-for%20public%20comments.pdf](http://meity.gov.in/sites/upload_files/dit/files/draft-rules-security%20of%20PPI-for%20public%20comments.pdf) [Accessed 10 April 2017].
- Reserve Bank of India (2015) Card Payments – Relaxation in requirement of Additional Factor of Authentication for small value card present transactions [Online] Available at: <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=9718&Mode=0> [Accessed 10 April 2017].
- Reserve Bank of India (2016a) Cyber Security Framework in Banks [Online] Available at: <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF> [Accessed 10 April 2017].
- Reserve Bank of India (2016b) Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions - Draft Circular Available at: [https://www.rbi.org.in/scripts/bs\\_viewcontent.aspx?Id=3235](https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=3235) [Accessed 10 April 2017].