Comments dated 20 March 2017 on the draft of the "Information Technology (Security of Prepaid Payment Instruments) Rules 2017" dated 8 March 2017 (Draft Rules) released by the Ministry of Electronics and Information Technology, Government of India (MeitY)

The Future of Finance Initiative (**FFI**) is housed within the IFMR Finance Foundation (**IFF**)[1] 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.

Our comments in response to the Draft Rules are presented in two sections below. In the first section titled "I. Overarching Comments", we raise two broad points on (1) extending the data protection principles consistently to avoid regulatory gaps, and (2) the need for regulatory coordination to avoid dual regulation, mitigate potential capacity constraints for MeitY and any adverse impact on the ease of doing business for pre-paid instrument (**PPI**) issuers. In the second section titled "II. Rule-Specific Comments", we provide rule-by-rule feedback on particular provisions of the Draft Rules.

SECTION I. OVERARCHING COMMENTS

1. **The Draft Rules reflect MeitY's progressive approach in solving customer data protection and privacy concerns. They must be extended consistently to all financial service providers to overcome any regulatory gaps.**

   We welcome the renewed focus on the protection of personal data and customer privacy reflected in the Draft Rules. In particular we welcome the provisions mandating that PPI issuers need to put in place strong privacy policies (as noted in Rule 4 of the Draft Rules), and the expansion of the scope and protections offered to customers whose personal data is collected by PPI issuers (Rules 7 to 10 of the Draft Rules).

   We are supportive of the need to extend these protections consistently for completeness (as detailed below) since there is a chance they could create certain regulatory gaps and customer risks in their current form.

1.1. <u>The Draft Rules while incorporating some of the key (and internationally recognised) data protection principles can benefit from a more complete coverage of these principles</u>: We recommend that the privacy policy requirements in Rule 4 should be expanded to cover key data protection principles that are widely accepted. We have listed the data protection principles (and their definitions) under key international

[1] 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).

conventions at the Annexure. Rule 4 covers several of these principles including the Purpose Specification principle; the Use Limitation Principle and the Security Safeguards Principle (see the definitions for each in the Annexure). However, the following principles are not covered by Rule 4: the Collection Limitation Principle, Data Quality Principle, Openness Principle, Individual Participation Principle, Accountability Principle and the Principle of Lawful Processing (see the definitions for each in the Annexure).

Rule 4(2) would also benefit from the inclusion of particular protections on obtaining customer consent and other data protections, which we have detailed in item 2 in section II (Rule-specific Comments) below.

1.2. Variation between the Draft Rules and the pre-existing RSPP Rules (also issued under the IT Act) may result in divergent standards for different body corporates: Rule 4 of the Draft Rules repeats some of the privacy policy requirements under Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 issued by the Ministry of Communications and Information Technology, Government of India (**RSPP Rules**). However, the overlap while consistent in most parts, departs from the RSPP Rules in certain aspects (both on form and substance). For instance, Rule 7(c) together with Rule 10 of the Draft Rules have the effect of deeming all financial data of a PPI customer - including transaction history - to be sensitive personal data or information (**SPDI**) for the purposes of the RSPP Rules. As a result, PPI issuers will need to handle financial data ***including transaction history*** in accordance with the higher data protection standards required for SPDI.

Since the Draft Rules do not apply to other body corporates collecting transaction data (such as for e.g. (i) banks, (ii) personal finance apps that may or may not come under the protections provided by RBI's outsourcing guidelines or by guidelines of any of the other financial sector regulators, (iii) other body corporates that have access to financial transaction data but are outside the purview of RBI or these draft guidelines, (iv) entities that offer data broking services and so on), these entities will not need to extend the same protections to transaction history. Other body corporates will remain under the rubric of Rule 3(ii) of the RSPP Rules where financial data as a category of SPDI does not include transaction history. This risks creating a separate or new standard only for PPI issuers handling personal data, which is slightly different from all other types of body corporates subject to the Information Technology Act, 2000 (**IT Act**) requirements. From a customer protection perspective, this means that other entities providing digital payments (such as banks or payments banks) or accessing transaction history data (like personal finance apps, or others mentioned above) would offer a weaker standard of data protection than PPI issuers. We also note that the Committee on Digital Payments constituted by the Ministry of Finance, Government of India, in its report dated 9 December 2016 (Watal Committee, 2016) had recommended that payment service providers be allowed to access personal data of users "*based only on explicit consent basis*".

We therefore request MeitY to strongly consider extending these and additional requirements (discussed in paragraph 1.3 below) to all body corporates accessing customer financial data including transaction histories.

1.3. Key categories of customer financial data that are collected by entities providing financial products and services should also be protected under the Draft Rules and the RSPP Rules: The current data protection regime in India mandates higher standards of care only for a narrowly defined set of SPDI (see Rule 3 of the RSPP Rules). In this context, we make a case for considering coverage of all "non-public personal information" (**NPI**). We elaborate upon this below.

It is relevant to note that the U.S. Gramm-Leach-Bliley Act, 1999 (GLBA, 1999) defines NPI as any "*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*." 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 emerges 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. As recently noted by the European Securities and Markets Authority in the context of 'Big Data' (ESMA, 2016):

> "*The use of Big Data is likely to transform the way products and services are provided with benefits for consumers (in terms of products/services better tailored to consumers' needs, better quality or cost-effective services/products) and financial institutions (for instance in terms of more efficient processes and decision-making or better management of risks or fraud situations). At the same time, the use of Big Data could potentially also have an impact on consumers' access to products/services, raise issues around the processing of data and financial institutions' pricing practices (e.g. based on analytical data showing a customer's likely willingness to pay more, or demonstrating his/her inertia to switch products) or decision-making using Big Data technologies, the potential limitations or errors in the data and analytic tools, or security and privacy/ethical concerns, eventually leading to legal and reputational risks for financial institutions. Potential entry barriers in accessing Big Data technologies could also have negative implications on innovation and competition in the financial markets at the detriment of consumers' welfare.*"

The importance of providing data protection to NPI thus stems from the growing commercial relevance of such information in the digital economy and is keeping in tune with the approach taken by regulators across most jurisdictions such as the U.S.A., European Union[2] (GDPR, 2016) and Australia[3] (Privacy Act, 1988).We therefore submit that all NPI (as defined above) be treated as SPDI for the purposes of the IT Act. Additionally, we recommend that MeitY leapfrog ahead from among these jurisdictions, by enhancing the definition of NPI to

[2] Article 4(1) of the Regulation (EU) 2016/679 of the European Parliament (i.e., the General Data Protection Regulation) defines "personal data" as: "*any information relating to an identified or identifiable natural person*".

[3] Part II, Division 1 of the Privacy Act, 1988 defines "personal information" as "*information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not*".

"*personally identifiable financial information that any institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available*." By doing so, MeitY, that has a pivotal role to play in the success of India's digital transformation, can provide comprehensive protections for customers not just in today's context but into years ahead that are set to see unprecedented disruptions from the use of Big Data.

2. **Enactment of the Draft Rules could raise issues of dual regulation and capacity, adversely impacting the ease of doing business.**

We note that MeitY proposes to issue the Draft Rules relying on its competence under Section 10(d)[4], Section 43A[5] and Section 87(1)[6] of the IT Act. We note that these powers are being extended to specifically create rules only for PPI issuers. Whilst MeitY has the power to make these discreet rules, doing so is likely to create significant concerns around dual regulation and MeitY's capacity to monitor and penalise non-compliance, as discussed below.

We therefore call for regulatory coordination between MeitY and the Reserve Bank of India (**RBI**) to avoid dual/disparate regulation, and also address capacity constraints on monitoring and enforcement.

2.1. The RBI is actively regulating PPIs, including on aspects of security: The RBI is vested with authority to regulate PPI issuers in the country, under the Payment and Settlement Systems Act, 2007 (**PSSA**). Section 3[7] of the PSSA specifically designates the RBI as the authority for the regulation and supervision of payment systems. PPI issuers are regarded as an *operator of a payment system* or a *system participant* by the RBI under the provisions of the PSSA. The RBI has power to determine standards for payment systems to comply with, as well as the conditions subject to which system participants (including PPI issuers) can participate in funds transfers (see sections 10[8] and 18[9] of the

[4] Section 10(d) of the IT Act (Power to make rules by Central Government in respect of Electronic Signature) reads: "*The Central Government may, for the purposes of this Act, by rules, prescribe: … (d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments*".

[5] Section 43A of the IT Act (Compensation for failure to protect data) reads: "*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.*"

[6] Section 87(1) of the IT Act (Power of Central Government to make rules) reads: "*The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.*"

[7] Section 3(1) (*Designated authority and its Committee)* of the PSSA reads "*The Reserve Bank shall be the designated authority for the regulation and supervision of payment systems under this Act.*"

[8] Section 10(1) of the PSSA provides that: "*The Reserve Bank may, from time to time, prescribe … (c) the manner of transfer of funds within the payment system, either through paper, electronic means or in any other manner, between banks or between banks and other system participants; (d) such other standards to be complied with the payment systems generally; (e) the criteria for membership of payment systems including continuation, termination and rejection of*

PSSA). In accordance with this power, the RBI has been actively regulating PPI issuers in the country. The Draft Rules create provisions that could give rise to dual regulation and overlaps with existing regulation. Specifically, we note the following:

- *RBI Notification on Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers*: The RBI issued a notification on security and risk mitigation measures to PPI issuers in December 2016 (The Reserve Bank of India, 2016a) (**PPI Security Notification**). This notification required PPI issuers to carry out a special audit by the empanelled auditors of Indian Computer Emergency Response Team (**CERT-In**) and take immediate steps to comply with the findings of the audit report. The regulations recommend the appointment of a senior functionary to monitor the PPI issuer's security compliance and report to the RBI on a monthly basis. It also required PPI issuers to take active steps to mitigate risks and threats, and send a detailed action plan to the RBI's Department of Payment and Settlement System (**DPSS**) by 21 December 2016.

- *RBI Master Circular – Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India*: The RBI's Master Circular – Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India (Reserve Bank of India, 2016b) **(PPI Guidelines)** already mandates that PPI issuers put in place adequate information and data security infrastructure to prevent frauds (paragraph 13 of the PPI Guidelines).

2.2. The RBI is currently reviewing the PPI Guidelines, specifically with an eye on customer safety and security: The RBI is reviewing its stance on the regulation of PPI issuers, which has been deliberately moderate until now as mentioned in the RBI Vision 2018 document (Reserve Bank of India, 2016c). In June 2016, the RBI specifically noted that a comprehensive review of PPI Guidelines would be undertaken to address aspects on safety and security, risk mitigation measures, complaint redressal mechanism, forfeiture of unutilised balances, fraud monitoring and reporting requirements (Reserve Bank of India, 2016d). The RBI has already passed guidelines in June 2016, on Cyber Security Framework in Banks (The Reserve Bank of India, 2016e) (**Cyber Security Guidelines**) and is well placed to extend these rules to PPI issuers, creating consistency and regulatory harmony. In February 2017, the RBI set up an Inter-disciplinary Standing Committee to review the threats inherent in the existing/emerging technology; study adoption of various security standards/protocols; interface with

membership; (f) the conditions subject to which the system participants shall participate in such fund transfers and the rights and obligations of the system participants in such funds".

[9] Section 18 of the PSSA provides that: "*... 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 elating to payment systems.*"

stakeholders; and suggest appropriate policy interventions to strengthen cyber security and resilience (The Reserve Bank of India, 2016f). The knowledge of this Committee would have direct relevance for the updated PPI Guidelines as well.

2.3. MeitY is best placed to continue its role as the overarching standards setting body for issues relating to security and integrity of electronic transactions. Downstream regulators should take up the actual monitoring and enforcement of such standards: If notified, MeitY would need to undertake enforcement and monitoring of the Draft Rules. As an example, Rule 14 of the Draft Rules mandates the PPI issuers set up mechanisms to report cyber incidents, cyber security incidents and cyber security breaches – but it is unclear how this will be monitored or how the failure by PPI issuers to do so will be penalised. The notification of these Draft Rules could result in a large number of complaints arising in respect of PPIs, and it would be prudent for MeitY to be mindful of the capacity constraints for effective implementation of the Draft Rules.

While the current legal rubric for PPI issuers would benefit from enhanced customer protections and data protection standards as described in the Draft Rules, maintaining harmony with existing regulation will ensure that:

- customer data held across all digital payment players receives the same level of protections, and

- overlapping rules and dual regulation (with slightly varying obligations, thus requiring dual reporting and raising the costs of compliance) do not confuse the regulatory landscape and reduce the ease of doing business for the PPI market in India.

We therefore support regulatory coordination between MeitY and the RBI to ensure harmonious regulation. MeitY should also leverage the existing monitoring mechanism and capacity within the RBI, which is the authorising body for PPI issuers and consequently has multiple touch points for regulation with them. For instance, the DPSS continually receives audit and process flow compliance reports from PPI issuers, and is in charge of oversight of all payment systems in the country (RTGS, NEFT, CCIL, mobile banking, ATMs, and pre-paid instruments) (Reserve Bank of India, DPSS, 2017). DPSS is well poised to continue to discharge these responsibilities and scale up its functions in face of additional regulation.

MeitY's role – as the pre-eminent body to set overarching standards to ensure adequate integrity, security and confidentiality of electronic records or payments – would also be fulfilled by using sectoral regulators to undertake monitoring and enforcement duties. MeitY can then continue setting the standards that apply across the market for data security and protection, ensuring even and comprehensive regulation.

SECTION II. RULE-SPECIFIC COMMENTS

We have listed our item-wise comments in the table below, referenced against the corresponding rule of the Draft Rules.

Sl. No.	Reference	Comment
1.	Rule 2(e)	The definition of "cyber incident" is imprecise which may create applicability and enforcement issues for PPI issuers and MeitY respectively. For instance, the definition includes an event that "*…undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation.*" Additionally, this is at variance with the definition of "cyber incident" already in existence under the RSPP Rules.
2.	Rule 4	In addition to the matters mentioned in paragraph 1.2 above with respect to Rule 4, we also recommend the following changes with regard to the privacy policy requirements: - Rule 4(2)(a): To specify that PPI issuers need to obtain prior written consent of customers for collection of their information, - Rule 4(2)(b): To specify the precise uses of all customer information obtained or held by PPI issuers, - Rule 4(2)(c): To specify bright-line standards for determining the period of retention of customer information by PPI issuers, and - Rule 4(2)(e): To mandate the PPI issuers to provide prior written intimation to the concerned customers pursuant to a lawful request. This is to enable such customers to take recourse of legal remedies for prevention of such disclosure to law enforcement agencies, as is standard practice with similar provisions in other regulations.
3.	Rule 5	- We note that this provision appears to be redundant due to the technical audit required by the RBI under its PPI Security Notification. As noted in paragraph 2.1 above, the PPI Security Notification set out a range of security and risk mitigation measures (including a technical audit of PPI issuers) in December 2016. PPI Security Notification already includes (i) risk assessment and audit requirements (ii) monthly reporting obligations to the DPSS. The reporting requirement in Rule 5 is in fact less frequent ("at least once a year") than required under the

		PPI Security Notification. It is also unclear to whom such reporting needs be done by the PPI issuers. - Rule 5 therefore risks creating confusion for the regulated entities with the PPI Security Notification. It does not provide a clear format for the reporting described or the monitoring authority. It also exerts costs of over compliance and duplicate regulation on PPI issuers.
4.	Rule 6(4)	- We welcome MeitY's promotion of additional factor authentication (**AFA**) for initiating settlements through PPIs to the extent that it is aimed at safeguarding the integrity of the digital ecosystem as a whole for customers. We do note however that authentication requirements for payment transactions have traditionally been in the RBI's regulatory domain, pursuant to its responsibilities and authority under the PSSA. - In addition, we request additional clarity on the possible exemption of 'certain e-PPI issuers' from AFA requirements. Currently comparable regulation of Small Value Card Not Present (CNP) transactions by the RBI does not require recurring AFA, provided the card issuing bank provides the customers with the option of one time AFA (Reserve Bank of India, 2016g). Under those regulations, if the customer chooses a one-time AFA, they need not undergo recurring AFA for transaction values under INR 2,000. In addition, the authorised card network bears complete liability in events of security breach in this mode of transaction under those regulations. - In the absence of such safeguards in the proposed Rule 6(4), we submit that the discretion to exempt certain PPI issuers from AFA may best be reserved.
5.	Rule 7, 8, 9, 10	We welcome the expansion of the categories of customer information for which protections are granted under these Rules. We reiterate the point that similar protections should be mandated not just for PPI issuers but also all other entities that hold such information from individuals, by expanding these requirements in the RSPP Rules.
6.	Rule 9(2)	- We welcome the inclusion of a provision placing controls on access to personal information once it has been collected by a particular entity. However, the standard applied to control access (i.e. that it should only be accessed by employees of a PPI issuer to confidential data should be on a "need-to-know" or "need-to-use" basis) is rather loose. - Instead, we submit that the requirement on entities collecting personal information should be to maintain a case-request log. This would require each employee to request access each time they want to access particular personal

		information of a customer, and record the time and reason for such access. - It is also noted that the access control requirements in this proposed Rule apply to "confidential data" which is not a defined term in the Draft Rules. The reference should instead be made to "personal data".
7.	Rule 11	We request more clarity on the operationalising of end-to-end encryption of data exchanged between communicating parties, as mandated in Rule 11. A decision to encrypt data necessitates careful consideration of which kind of data exchanges ought to be encrypted, given cost of encryption and monitoring.
8.	Rule 15	- We welcome the inclusion of a provision placing obligations on PPI issuers to keep customers informed of all information relating to the security of PPIs, initiation of payments and security procedures (Rule 15(4)). We however note that there appears to be an overlap with the RBI's PPI Guidelines which place requirements on PPI issuers to disclose all important terms to customers (see paragraph 14 of the PPI Guidelines). - Separately we note that the Rule calls for PPI issuers to put in a place a mechanism to obtain assistance relating to their questions and complaints regarding the use of PPIs (Rule 15(5)). This seems unconnected to the stated objective of these rules as stated in the objects section of the Draft Rules i.e. "*to ensure adequate integrity, security and confidentiality of electronic payments effected through prepaid payment instruments*".
9.	Rule 16	- While grievance redressal is an important aspect of customer protection, the PPI Guidelines already provide that: • 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). • customers of bank PPI issuers can approach the Banking Ombudsman for grievance redressal. By setting up parallel and different requirements, the Draft Rules can create confusion for the regulated entities with the PPI Guidelines. It also exerts costs of over compliance and duplicate regulation on PPI issuers, and could confuse customers to the extent that dual routes to complaints resolution are put in place by PPI issuers seeking to

		comply with both regulations. - In contrast, this Rule does not impose any reporting requirement for non-bank PPI issuers and takes away the ability of customers of bank PPI issuers to avail the Banking Ombudsman Scheme of the RBI. In light of this, we recommend that the Draft Rules be updated to refer to the existing grievance redressal provisions in paragraph 14 (*Customer Protection* issue) of the PPI Guidelines, to avoid dual regulation and regulatory confusion.

ANNEXURE (Data Protection Principles under Key International Conventions)

Note: The table indicates 'Y' where the relevant principle is included in the international conventions listed and 'N' if not.

AUC	*African Union Convention On Cyber Security And Personal Data Protection, EX.CL/846(XXV) (2014)*
OECD/G20	*G20/OECD Task Force On Financial Consumer Protection - Effective Approaches To Support The Implementation Of The Remaining G20/OECD High-Level Principles On Financial Consumer Protection (2014)*
EU GDPR	*European Union General Data Protection Regulation (Regulation (EU) 2016/679 (2016)*
APEC	*Asia-Pacific Economic Cooperation Privacy Framework, APEC#205-SO-01.2 (2005)*

Principle	Description	AUC	OECD/ G20	EU GDPR	APEC	Draft Rules
Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (the person to whom the information pertains and from whom information is collected).	Y	Y	Y	Y	N
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	Y	Y	Y	Y	N
Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	Y	Y	Y	Y	Y
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: (a) with the consent of the data subject; or	Y	Y	Y	Y	Y

	(b) by the authority of law.					
Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	Y	Y	Y	Y	Y
Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller (the person who collects the data and determines the manner of its use).	Y	Y	Y	Y	N
Individual Participation Principle	An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	N	Y	Y	Y	N

Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.	Y	Y	Y	Y	N
Principle of lawful processing	The data processor must: (a) have legitimate grounds for collecting and using the personal data; (b) not use the data in ways that have unjustified adverse effects on the individuals concerned; (c) be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data; (d) handle people's personal data only in ways they would reasonably expect; and (e) make sure it does not do anything unlawful with the data.	Y	N	Y	Y	N

BIBLIOGRAPHY

- European Securities and Markets Authority, 2016, Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions [Online] Accessible at https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf [Accessed 20 March 2017].

- General Data Protection Regulation, 2016 [Online] Accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 20 March 2017].

- Reserve Bank of India (2016a) Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers, December 09, 2016, RBI/2016-17/178 DPSS.CO.OSD.No.1485/06.08.005/2016-17 [Online] Available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI17870D26479352A448E98CBF5E7C8652C29.PDF [Accessed 20 March 2017].

- Reserve Bank of India (2016b) Master Circular – Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India, July 01, 2016, RBI/2016-2017/16 DPSS.CO.PD.PPI.No.01/02.14.006/2016-17 [Online] Available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/16MC9102DB7D5FE742CCB5D0715A77F6666E.PDF [Accessed 20 March 2017].

- Reserve Bank of India (2016c) Payment and Settlement Systems in India: Vision-2018, June 23, 2016, [Online] Available at: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/VISION20181A8972F5582F4B2B8B46C5B669CE396A.PDF [Accessed 20 March 2017].

- Reserve Bank of India (2016d) Temporary suspension in grant of Authorisations for Pre-paid Payment Instrument (PPI) issuance, September 09, 2016, Press Release: 2016-2017/588 [Online] Available at: https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=37965 [Accessed 20 March 2017].

- Reserve Bank of India (2016e), Cyber Security Framework in Banks, June 02, 2016, RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16 [Online] Available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF [Accessed 20 March 2017].

- Reserve Bank of India (2016f) Reserve Bank Establishes an Inter-disciplinary Standing Committee on Cyber Security, February 28, 2017, Press Release: 2016-2017/2303 [Online] Available at: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR230352D612E69EC045D5A86CFA85D10094C4.PDF [Accessed 20 March 2017].

- Reserve Bank of India (2016g), Card Not Present transactions – Relaxation in Additional Factor of Authentication for payments up to ₹ 2000/- for card network provided authentication solutions, December 06, 2016, RBI/2016-17/172 DPSS.CO.PDNo.1431/02.14.003/2016-17 [Online] Available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10766&Mode=0 [Accessed 20 March 2017].

- Reserve Bank of India, DPSS (2017), Functions of DPSS, RBI [Online] Accessible at https://www.rbi.org.in/commonman/English/Scripts/Departments.aspx#DPSS1 [Accessed 20 March 2017].

- U.S. Gramm-Leach-Bliley Act, 1999 [Online] Accessible at https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf [Accessed 20 March 2017].

- U.S. Privacy Act, 1988 [Online] Accessible at https://www.legislation.gov.au/Details/C2016C00979 [Accessed 20 March 2017].

- Watal Committee, 2016, Committee to review the framework related to Digital Payments [Online] Accessible at http://finmin.nic.in/reports/watal_report271216.pdf [Accessed 20 March 2017].