20 March 2017

COMMENTS ON DRAFT INFORMATION TECHNOLOGY (SECURITY OF PREPAID PAYMENT INSTRUMENTS) RULES 2017

I. Background

The Ministry of Electronics and Information Technology (MeitY) released the Draft Information Technology (Security of Prepaid Payment Instruments) Rules 2017 (Rules) to ensure adequate integrity, security and confidentiality of electronic payments effected through prepaid payment instruments (PPIs). CUTS International (www.cuts-international.org) is a not-for-profit, non-partisan economic policy research and advocacy organisation which has been working in the field of digital finance and payments for a significant period.

Following are CUTS' comments on the Rules:

II. Comments by CUTS

1. Compliance with Pre-legislative Consultative Policy of the Government of India (Policy)

The Government of India has issued a Policy on prior consultations on legislations and rules drafted by the government.[1] The Policy requires government to place in public domain explanatory notes explaining key legal provisions of draft legislations or rules in a simple language (clause 5). In addition, brief justification, broad financial implications, estimated impact and other relevant details are required to be published in public domain (clause 2).

The MeitY has not published any details other than the draft rules. Without important details, the task of providing comprehensive comments is difficult. It is thus suggested that relevant important details in accordance with Policy are released in public domain.

2. Expanding the scope of customer

The Rules define customer as person who acquires prepaid payment instrument (PPIs). PPIs facilitate payments between individuals and more often than not, the e-PPI issuer will have access to sensitive details of individuals/ entities to whom recurring payments are made by persons who acquire the PPIs. e-PPI issuers must be responsible to protect

[1] The policy is available at http://lawmin.nic.in/ld/plcp.pdf

sensitive details of such persons, who are not directly their consumers, but whose sensitive information are available with them. All provisions of the Rules which empower and protect direct consumers of PPIs, must be applicable to the indirect consumers (recipients) as well.

3. Remove contingency in 'cyber security incident' and 'cyber security breach'

According to rule 2(f), any real or suspected adverse event in relation to cyber security that **violates an explicitly or implicitly applicable security policy** can be treated as 'cyber security incident' only when such event results in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation. In other words, violation of applicable security policy is not enough, but subsequent result in form of unauthorised access etc. is relevant for e-PPI issuer or CERT-In to take necessary action. This contingency should not be necessary and the e-PPI issuers or CERT-In must be activated as soon as they detect violation of security policy, and must be required take appropriate actions.

Similarly, according to rule 2(g), any **unauthorised acquisition** by a person of data or information maintained in a computer resource can be called as 'cyber security breach' only when such acquisition compromises the confidentiality, integrity or availability of information maintained in a computer resource. In other words, mere unauthorised acquisition does not trigger the necessary responses required in case of cyber security breach. Such inability might restrict the ability of e-PPI issuer to prevent and block the potential compromise of confidentiality, integrity or availability of said data and information. Consequently, it is necessary that e-PPI issuers and CERT-In are activated even when there no compromise, but merely unauthorised acquisition.

4. Loading of PPI

The definition of PPI under clause 2(n) assumes that value stored in a PPI can represent the value paid for by the holders of cash, debit to a bank account or by a credit card. It does not envisage loading of a PPIs by through other PPIs. In other words, it does not envisage direct and complete interoperability among PPIs.

While at present, PPIs are not directly and completely interoperable, this could change in near future. Consequently, the clause need to storage of value in a PPI through debit to another PPI.

5. Scope of Issuers

The Rules are applicable to only persons 'authorised' by RBI to operate payment system issuing PPI. In reality, several persons might be operating payments systems and issuing

PPIs without RBI approval. This is a real possibility, given limited monitoring and supervision capability of RBI.

Consequently, the Rules should be applicable to any person operating payment system issuing PPI.

6. Information security policy and need for activity based regulation

The primary business of e-PPI issuer is to facilitate digital payments. Banks, while conducting several other transactions, are also in the business of facilitating payments. The information security standards and other regulations applicable to payments business of all authorised entities should be similar in nature, despite difference in other businesses carried on by such entities.

Consequently, there is a need to move towards activity based regulation and ensure parity of payments related regulation (including information security policy) for entities authorised to provide digital payments services.

7. Strengthening the Rule on Privacy Policy

The draft rules under Rule 4 mention several important considerations which would govern the privacy policy of PPIs (apart from any other details as may be specified by Central Government). However, there is still scope for strengthening the said rule by including the following details:

- PPIs should also be mandated to mention the **purpose** for which information is being collected, which should be explicitly mentioned at the time of collection. This would be a precursor to Rule 4(2)(b).[2]
- Consumers should also have a ready **option to opt out of the policy** and request deletion and retention of private information. This option should be made explicitly visible to the consumer in the policy.
- Privacy policies should be mandated to **attain informed and meaningful consent.** This not only includes informing the consumer about the collected information as mentioned in Rule 4(2)(a), but also regularly informing and obtaining his consent regarding any **updates in the policy** which affects the collected information. In addition, the default option should be 'no sharing' of sensitive information, and the customer should have the option to select the kind /extent of information she wants to share and the entities with which the information can be shared.

[2] OECD, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), available at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

- On generation of every new kind of information or an additional entity with which the information could be potentially shared, the customer should be prompted with an alert about such sharing before the completion of transaction. Customer should have the option to decline sharing of information. Customer should also have the right to opt-out from unsolicited offers even when information is shared.
- The privacy policy must be available in all scheduled languages and also in picture and audio/ video format for consumers.
- Change in policy terms must be communicated and consent must be obtained afresh on each change *(Comment taken from submission by Cashless Consumer)*.
- The website of e-PPI issuer should host all versions of versions of privacy policy and period of applicability of each version of the policy. *(Comment taken from submission by Cashless Consumer)*.
- Clarify and specify "law enforcement agencies" with department / rank of officials with whom the information must be shared. In the past, with 66A of the IT Act, rampant misuse of power had been a notable example, where Supreme Court before scrapping allowed only enforcement officers beyond DSP to be eligible to register a case. Since access to payment information is sensitive, private, access to information by law enforcement agencies must follow well defined process, with sufficient systemic checks to prevent abuse of power by people in law enforcement agencies. *(Comment taken from submission by Cashless Consumer)*.
- Expand contact details of grievance officer to phone number (with timings to contact), email address, physical address. *(Comment taken from submission by Cashless Consumer)*

8. Risk Assessment

Rule 5(2) requires every e-PPI issuer to review security measures at least once a year. Given the dynamic nature of the industry, ongoing developments, every e-PPI issuer must be required to conduct summary review of its security measures every quarter and publish a report of its security in public domain. The report should explain the security features, changes, and any vulnerability identified in simple and clear language.

Further, risk assessment should be mandated after **all** security incidents and not merely **major** security incidents. The type of breach; extent of damage, if any; details of assessment conducted; and controls put in place to prevent such breach in future.

9. Customer identification and authentication and the need to avoid regulatory ambiguity

Rule 6(3) mentions the requirement of multiple-factor authentication to be followed whenever a customer initiates a payment against the value stored on the PPI. Currently, RBI regulations allow single factor authentication for low value transactions and thus there is a conflict between this provision and RBI regulation. In addition, PPIs are regulated by RBI, which has the power to issue security related regulations for them. Existence of multiple regulatory agencies often results in regulatory overlap and ambiguity, which must be avoided.

In addition, this mandate can hamper seamless transactions that several PPIs currently offer and also act as **barriers for future innovations** in this space, as multiple factor authentications are only one of the mechanisms to secure transactions. There could be several other low cost and user friendly mechanisms which promote security. PPIs should be allowed to innovate authentication mechanisms as long as they ensure that security is not breached. Similarly, consumers must have the right to different from different mechanisms and set different levels of security depending on indicators (such as amount, recipient etc) they might be comfortable with.

Further, rule 6(5)(a) provides for confidentiality of authentication data. This should be maintained despite operationalisation of the Central KYC registry which is envisaged as one store room for all KYC records of a customer. No service provider should be allowed to access customer identification and authentication details without informed and express customer consent.

Rule 6(5)(c) requires specification on maximum number of failed authentication attempts and provision of temporary blockage of account. However, if authentication is failed owing to unavailability of internet access of unfair rejection by service provider, customer must not be penalized. On the contrary, it should be compensated for failure to access its account for reasons beyond its control.

10. Personal information

Email address, physical address, customer photograph, unique number (aadhar number/ pan etc) of customers should be included in the scope of personal information. All information related to the customer should be by-default considered as personal information, unless other expressly exempted after express and informed consent of the consumer.

11. Reporting of cyber incidents

Notification to consumers about cyber security incidents or breaches should be mandatory in all cases. Also, reports filed with CERT-In should be available in public domain.

12. Accountability of PPI in case of fraud by agents

Under Rule 15, PPIs should also be assigned the responsibility to **inform the consumer** about accountability in case of any direct loss due to fraud by agents, employees, and third party service providers and for third party fraud caused by a reasonably preventable security breach.[3] The user should also be informed immediately about any suspected fraud. This would substantially strengthen the directive of the Rules regarding accountability and transparency of PPIs.

13. Grievance redressal

The resolution of grievance should be possible within seven days of lodging of complaint. Consumers should be in a position to escalate the matter to government authorities in case of failure in doing so.

In addition, the Grievance Officer role defined in this draft should related to cyber security and rules mentioned here and must be separate from grievance officer for payment related issues whose role must be defined by RBI or soon to be set up Payments Regulatory Board at the earliest. *(Comment taken from submission by Cashless Consumer)*

14. Dispute Resolution through digital means

Experience from other jurisdictions demonstrates that effective recourse mechanisms for users (that function in a digital environment) are critical to building users' trust in using financial services.[4] Thus, in addition to the mandatory grievance redressal mechanism[5], PPIs should also be required to **establish an independent third party dispute resolution mechanism (including through digital means)**.[6] The dispute resolution mechanism would be established to handle cases where users believe that complaints were not addressed adequately by the service provider/PPI. This is especially relevant for users in rural/far-fetched areas who do not have easy and cost-effective access to the formal judicial recourse mechanisms.

15. Security Standards

Internationally accepted security standards must be adopted by e-PPI issuers.[7]

****

[3] Better than Cash Alliance, *Responsible Digital Payments Guidelines* (2016), p.17 available at http://www.uncdf.org/sites/default/files//Documents/btca-responsible_digital_payments_guidelines_and_background.pdf

[4] Ibid., at p.8

[5] As suggested under Rule 16.

[6] Supra note 3. CUTS International runs a Consumer Care Centre to help consumers resolve greivances.

[7] For instance, see security standards recommended by ITU. Available at http://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf