Draft Prepaid Payment Instruments Rules, 2017: An Analysis

Introduction

The advent of demonetization has given a push towards a digitalized and cashless economy, promoting mobile wallets and electronic payments. With the accelerated use of electronic payment mechanisms and enormous personal and financial data shared on the applications, the central government has announced the draft Information Technology (Security of Prepaid Payment Instruments) Rules 2017 ("**Draft PPI Rules**"), under the Information Technology Act, 2000 ("**IT Act**"). The purpose of the said rules is to ascertain the integrity, security and confidentiality of the prepaid payment instrument(s) ("**PPI**").

This newsletter evaluates and comments on key provisions of the Draft PPI Rules, in light of the corresponding Master Circular by Reserve Bank of India ("**RBI**") on PPI[1] ("**Master Circular**") and the data protection rules under the IT Act[2] ("**SPDI Rules**").

1. Key Provisions

1.1 Definition of PPI

In the Draft PPI Rules, PPI is defined as a payment instrument for purchase of goods and services, including funds transfer, against the value stored in the instrument.[3] The definition is identical to the one provided in Clause 2.3 of the Master Circular. Currently, the definition only takes into account the payment into PPI using cash, debit to a bank account and credit card. Potentially, the definition may have to be revisited in view of technological progress, if other modes of adding money to a PPI, such as inter-PPI transfer are introduced. A wider definition of PPI will perhaps be more useful to avoid a regulatory gap in the future.

1.2 Security standards and practices

The Draft PPI Rules require an issuer to provide for a dual security system, an information security policy for the security of its payment system, and reasonable security practices and procedures for the financial data of the customers.[4] In addition, it's essential to adhere to the security measures provided in the Master Circular, wherein the issuer should have an adequate information and data security infrastructure.[5]

The three set of regulations stated above provide for three different security standards. These security standards suffer from certain overlap. For instance, the reasonable security practices and procedures under the SPDI Rules include the "*managerial, technical, operational and*

[1] Master Circular on Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India, dated July 01, 2016
[2] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[3] See Rule 2(1)(n) of Draft PPI Rules
[4] See Rule 3 read with rule 17 of the Draft PPI Rules and Rule 8 of SPDI Rules
[5] See Clause 13.1, Master Circular

physical security measures";[6] the information security policy under the Draft PPI Rules may fall under the operational and technical security measures of the reasonable security practices and procedures. The security measures under the SPDI Rules are wide-ranging; therefore, a separate information security policy seems unnecessary.

Perhaps, a better approach will be to provide for comprehensive set of security standards and policy or, alternatively, synchronize the regulations provided under the Master Circular, SPDI Rules and the Draft PPI Rules. For example, the Master Circular can provide that the information and data security infrastructure of the issuer will be considered adequate if it follows the practices and procedures under the SPDI Rules.

1.3 Personal information

Rule 7 of the Draft PPI Rules define personal information to include "*information collected from the customer or elsewhere at the time of issuance of the pre-paid payment instrument..*" and "*information collected during use of the payment system...*".The SPDI Rules state that personal information means "*information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*". Financial information is also covered under sensitive personal data or information under the SPDI Rules.[7]

Draft PPI Rules basically reiterate what is already covered under the SPDI Rules, albeit, in a different language. A standardized definition of personal information, as information that can be identified with a natural person, instead of varying definitions that quintessentially indicates the same meaning of personal information, might have been a better option.

1.4 Cyber incident and cyber security incident

Draft PPI Rules require an issuer to have a mechanism to deal with cyber incident and cyber security incident. The former means any real or suspected adverse event, likely to cause or cause an offence or contravention, harm to critical functions across public and private sector, by impairing the integrity, confidentiality, availability of the electronic information system and services. Such impairment should result in an unauthorized access or use of the computer resource or denial of service or disruption, change to data or information without authorization, or it should threaten public safety, undermine public confidence, have a negative effect on the economy and diminish the security posture of the nation.[8] Cyber security incident on the other hand means any real or suspected adverse event relating to cyber security that violates the applicable security policy. Such violation should result in an unauthorized access or use of the computer resource or denial of service or disruption, change to data or information without authorization.[9]

In short, cyber incident and cyber security incident indicates adverse event likely to result in an unauthorized access. It is interesting to note that this same definition of cyber security incident is provided under Rule 2(1)(d) of SPDI Rules as "cyber incident".

[6] See Rule 8, SPDI Rules
[7] See Rule 3, SPDI Rules
[8] See Rule 2(1)(e), Draft PPI Rules
[9] See Rule 2(1)(f), Draft PPI Rules

The definition of cyber incident is wide enough to include cyber security incident. A separate definition of the latter seems unnecessary. Further, the two definitions should not be contingent on unauthorized access, but an attempt to cause such an event should be sufficient. Section 84C of the IT Act provides that even an attempt to commit an offence under the IT Act is punishable. In light of this, occurrence of real or suspected adverse event that violates security policy or causes an offence should be adequate to constitute cyber incident/cyber security incident.

Further, such incidents are required to be reported to the national Computer Emergency Response Team ("**CERT-in**").[10] In addition, the recent draft master direction by RBI on PPI requires reporting to RBI of such incident.[11] A consolidated reporting requirement to one entity may be more helpful. Interestingly, there is no mandatory requirement of reporting such incidents to the customer,[12] which should be made obligatory.

1.5 Grievance redressal mechanism

Rule 16 of Draft PPI Rules require an issuer to designate a grievance officer for receiving complaints from the customer, and publish the details of the grievance officer on its website along with the procedure for making the complaint. An almost identical provision is specified under Rule 5(9) of SPDI Rules.

Further, in an inevitable overlap, Clause 14.2 of Master Circular also provides for the grievance redressal mechanism. It states that "*the non-bank PPI issuer shall put in place an effective mechanism for redressal of customer complaints along with escalation matrix and publicise the same for the benefit of customers....*"

The aforementioned provisions have the propensity to put an issuer in a quandary over the redressal mechanism that it ought to follow. While the Master Circular specifies the requirement of an escalation matrix, the draft PPI Rules limits it to just having a grievance officer. PPI issuer should be mandated to provide an inbuilt escalation mechanism, for effective grievance resolution without approaching the courts.

Further, the nature of grievances for which customers can approach a grievance officer is unclear. The draft PPI Rules can possibly also incorporate a suggestive list of grievances for which the grievance officer can be approached.

1.6 Authentication of information, traceability and retention of information

Apart from overlap with the SPDI Rules and Master Circular, Draft PPI Rules *per se* don't promise a comprehensive protection to PPI or promote ease of business. For instance, Rule 6(2) states that an issuer must adopt multiple factor authentication process when a customer tries to make a payment for goods and services from the value stored in a PPI. The popularity of a PPI, like a mobile wallet lies in the ease of use; unlike internet banking or debit card payment, it doesn't have multi-layered authentication. For example, payment using a mobile

[10] See Rule 14 of Draft PPI Rules
[11] See Rule 15.7, Draft Master Directions on Issuance and Operation of Prepaid Payment Instruments in India dated March 20, 2017
[12] See Rule 14(3), Draft PPI Rules

wallet like Paytm does not require one time password or the need to give the debit or credit card detail. A multiple factor authentication may make the usage of PPI cumbersome and hinder seamless transactions, especially for low value transactions. Multiple layer authentications by a mobile wallet to pay for taxi aggregator services that are frequently used may not be customer friendly.

Rule 12 further stipulates that interactions with customers or other service providers can be "*appropriately traced*", specifically with regard to the access to payment accounts and initiation of payment. The meaning of appropriately traced is unclear. Further, the rule does not specify the purpose or intent behind tracing such details.

Close on the heels of the provision of traceability, Rule 13 provides for the retention of data relating to electronic payment for a specified period, that may be specified by the central government. The nature of data that can be retained and the rational for such retention is not clear, further the duration for retaining information is yet to be specified.

Conclusion

The Draft PPI Rules coincide repeatedly with SPDI Rules and the Master Circular that may cause confusion among the issuers, and instead of promoting stringent protection of data and information, lead to non-compliance with multiple regulations. An alternative approach would be to synchronize the applicable sectoral regulations. For instance, the draft PPI Rules could perhaps instead of requiring a separate security policy, refer to security measures under the SPDI Rules, or, for reporting of cyber incidents, instead of dual reporting to CERT-in and RBI, provide for one reporting entity, either RBI or CERT-in, as the case may be. In addition, the provisions like data retention and grievance redressal needs to be more specific in nature. In summation, the introduction of the Draft PPI Rules is a commendable move in the right direction, but it is far from being sufficient.

Author
Srishti Aishwarya