KHAITAN &CO
Advocates since 1911

NEWSFLASH

ERGO
Analysing developments impacting business

RELEASE OF DRAFT RULES FOR SECURITY OF PREPAID PAYMENT INSTRUMENTS

2 May 2017

The Ministry of Electronics and Information Technology, on 8 March 2017, released the draft Information Technology (Security of Prepaid Payment Instruments) Rules, 2017 (Draft Rules), under the Information Technology Act, 2000 (IT Act), for public comments.

Background

The Draft Rules seek to provide a framework of security practices for 'electronic prepaid payment instruments', in view of the Government's recent efforts to promote a cashless economy post demonetisation and the resulting boost to digital payment systems in India.

According to the definition provided by the Reserve Bank of India (RBI), prepaid payment instruments or "PPIs" as they are commonly known, are "payment instruments that facilitate purchase of goods and services, including funds transfer, against the value stored on such instruments". PPIs are mainly governed by the provisions of the Payments and Settlement Act, 2007, and related guidelines and master circulars of RBI.

PPIs may be in physical or electronic form. Examples of physical PPIs include smart cards and payment vouchers, while mobile wallets and internet banking are examples of electronic PPIs. Unlike physical PPIs, in electronic PPIs, the payment account is accessed through electronic means.

Further, since electronic PPIs are digital/electronic in nature, they are additionally governed by the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (IT Rules), regarding cyber security and data privacy.

Despite the existing legal framework, owing to the inherent vulnerability of computer systems and mobile devices and the current surge in use of electronic PPIs, the Government has now sought to put in place additional mechanisms to augment the security of such digital payments. The Draft Rules have been issued with this perspective and applies largely to electronic PPIs.

Draft Rules and e-PPI Issuers

Electronic PPI issuer or e-PPI Issuer has been defined under the Draft Rules "as a person operating a payment system issuing pre-paid payment instruments to individuals / organizations … where the payment account is accessed through electronic means".

Under the Draft Rules, certain obligations in addition to those under the IT Rules are cast upon the e-PPI Issuer which are as follows:

- Protection of personal information: 'Personal information' (in relation to certain offences under the IT Act) will specifically include: (a) information collected directly from the customer 'or elsewhere' at the time of issue of PPI, like customer's name, address and telephone number (b) any information collected during use of PPI system operated by Issuer and (c) authentication data like any information submitted by customer at the time of authentication for verifying his/her identity for accessing account or making payment. This personal information will be required to be protected. The ambit of personal information has been widened to include any information collected from the customer 'or elsewhere'. It may be noted that the provision uses the term Issuer instead of e-PPI Issuer, creating ambiguity.

- Adherence to an Information Security Policy: e-PPI Issuers must develop and adhere to an information security policy complying to technical standards specified by the Government.

- Publication of Privacy Policy: Every e-PPI Issuer is required to publish on its website and mobile application, a privacy policy for use of the payment systems, in simple language. The proposed privacy policy requirements are similar to those under the IT Rules, but under the Draft Rules it also includes any information directly and otherwise collected from the customer.

- Contractual arrangements: The Draft Rules also requires that e-PPI Issuers to contractually ensure that merchants handling any authentication data to have security measures in place to protect personal information.

- Customer Identification and Authentication: The Draft Rules requires proper authentication of a customer by e-PPI Issuer both at the time of issue of PPI and at the time PPI is accessed by customer or when a payment is initiated. There could be certain exemptions that the Government may propose for multiple authentications depending on the amount and nature of transaction.

- Risk Assessment: e-PPI issuers are required to carry out risk assessment to identify and assess risks associated with the security of the payment systems and review such measures at least once a year and after any major security incident or before any major change in its infrastructure.

Khaitan Comment

Security and confidentiality of financial transactions and consumer data is a key element in enhancing consumer confidence in digital transactions and making the drive towards cashless economy a success. The Draft Rules seem to be a step in that direction, but it is hoped that clarity on certain aspects related to its applicability will be properly addressed in the final version.

Further, as e-PPI Issuers must develop privacy policies for any information collected from customers or otherwise, it makes the scope of the privacy policy wide and ambiguous.

Different e-PPI Issuers may interpret information collected from customer 'or elsewhere' differently.

Additionally, the Draft Rules do not propose the minimum level of security and data protection measures that e-PPI issuers must pass on contractually to their merchants. Unless appropriately modified, it may result in incongruity in the practices followed by e-PPI Issuers and merchants and a threat to the information available with merchants.

We look forward to the final version of the rules in relation to security of e-PPIs and will share an update on it once published.

- *Harsh Walia (Associate Partner) and Abhinav Chandan (Principal Associate)*

For any queries please contact: editors@khaitanco.com

Mumbai
One Indiabulls Centre, 13th Floor
Tower 1 841, Senapati Bapat Marg
Mumbai 400 013, India

T: +91 22 6636 5000
E: mumbai@khaitanco.com

New Delhi
Ashoka Estate, 12th Floor
24 Barakhamba Road
New Delhi 110 001, India

T: +91 11 4151 5454
E: delhi@khaitanco.com

Bengaluru
Simal, 2nd Floor
7/1, Ulsoor Road
Bengaluru 560 042, India

T: +91 80 4339 7000
E: bengaluru@khaitanco.com

Kolkata
Emerald House
1 B Old Post Office Street
Kolkata 700 001, India

T: +91 33 2248 7000
E: kolkata@khaitanco.com