**Government of India**

**Ministry of Electronics and Information Technology**

**Information Technology (Security of Prepaid Payment Instruments) Rules 2017 –Draft**

In exercise of powers conferred by clause (d) of section 10 and section 43A read with sub-section (1) of section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules to ensure adequate integrity, security and confidentiality of electronic payments effected through prepaid payment instruments, namely:—

1. **Short title and commencement**.—(1) These rules may be called the Information Technology (Security of Prepaid Payment Instruments) Rules, 2017.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions**.—(1) In these rules, unless the context otherwise requires,—

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "authentication" means verifying a customer's identity based on authentication data using one or more elements categorised as knowledge, possession and inherence;

(c) "authentication data" means any information submitted by a customer at the time of authentication, and includes passwords, OTPs, Aadhaar numbers, biometric attributes, or any other data that may be used for authentication purposes;

(d) "customer" means a person who acquires a prepaid payment instrument;

(e) "cyber incident" means any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

(f) "cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting 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;

(g) "cyber security breach" means unauthorised acquisition by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(h) "electronic pre-paid payment instrument issuer" or "e-PPI issuer" means a person operating a payment system issuing pre-paid payment instruments to individuals/ organisations under authorisation from the RBI under the Payment and Settlement

Systems Act 2007, where the payment account is accessed through electronic means;

(i) "Indian Computer Emergency Response Team" or "CERT-In" means the Indian Computer Emergency Response Team set up under sub section (1) of section 70(B) of the Act;

(j) "multiple factor authentication" means authentication based on the use of two or more elements categorised as knowledge, possession and inherence, as specified by the Central Government;

(k) "password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

(l) "payment account" means an account of the customer that is used to access the value stored on a pre-paid payment instrument;

(m) "payment system" shall have the same meaning as ascribed to it in the Payment and Settlement Systems Act, 2007;

(n) "pre-paid payment instrument" or "PPI" means a payment instrument that facilitates purchase of goods and services, including funds transfer, against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card. The pre-paid instruments can be issued as smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers and any such instrument which can be used to access the pre-paid amount;

(o) "Issuer" means a person operating a payment system issuing pre-paid payment instruments to individuals/ organisations under authorisation from the RBI under the Payment and Settlement Systems Act 2007.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. **Information security policy**.—Every e-PPI issuer shall develop an information security policy for security of the payment systems operated by it, in accordance with these rules and any standards specified by the Central Government for this purpose under Rule 17.

4. **Privacy policy**.—Every e-PPI issuer shall have in place and publish on its website and mobile applications the privacy policy and the terms and conditions for use of the payment systems operated by it in simple language, capable of being understood by a reasonable person.

(2) The privacy policy shall include the following details, namely:—

(a) the information collected directly from the customer and information collected otherwise;
(b) uses of the information;
(c) period of retention of information;
(d) purposes for which information can be disclosed and the recipients;
(e) sharing of information with law enforcement agencies;
(f) security practices and procedures;

(g) name and contact details of the Grievance Redressal officer along with mechanism for grievance redressal;
(h) any other details as may be specified by the Central Government for this purpose.

5. **Risk assessment and risk control.—**(1) Every e-PPI issuer shall carry out risk assessment to identify and assess the risks associated with the security of the payment systems operated by it.

(2) Every e-PPI issuer shall review the security measures at least once a year, and after any major security incident or breach or before a major change to its infrastructure or procedures.

(3) Every e-PPI issuer shall implement security measures in accordance with the information security policy to mitigate the identified risks.

6. **Customer identification and authentication.**—(1) Every e-PPI issuer shall ensure that customers are identified through adequate due diligence procedures at the time of issuance of a pre-paid payment instrument, in accordance with applicable guidelines issued by the Reserve Bank of India.

(2) The e-PPI issuer shall apply appropriate procedures for authentication where a customer accesses his payment account online.

(3) The e-PPI issuer shall adopt multiple factor authentication where a customer initiates a payment against the value stored on the pre-paid payment instrument.

(4) The Central Government may, by notification, exempt e-PPI issuers from the requirement of multiple factor authentication in specified cases depending on the amount, nature of transaction, risk involved and like factors.

(5) The procedure for authentication shall include mechanisms to:

(a) protect the confidentiality of authentication data;

(b) limit the maximum time allowed to the customer to access his payment account online;

(c) specify the maximum number of failed authentication attempts that can take place consecutively within a given period of time and after which the access to an online payment account or the initiation of a payment is temporarily blocked;

(d) protect communication sessions against capture of data transmitted during the authentication procedure or manipulation of unauthorised parties; and

(e) prevent, detect and block fraudulent payments before the e-PPI issuer's final authorisation.

7. **Personal information.—**The following information shall be deemed to be personal information for the purpose of Section 72A of the Act—

(a) information collected from the customer or elsewhere at the time of issuance of the pre-paid payment instrument, including name, address, telephone number of the customer;

(b) information collected during use of the payment system operated by the

Issuer;

(c) financial data of the customer, including bank account details, debit card or credit card or other payment instrument details, transaction history;

(d) authentication data; and

(e) any other information as may be notified by the Central Government.

8. **Security of personal information.**—(1) Every e-PPI issuer shall adopt security measures to protect the security, confidentiality and integrity of the personal information referred to in Rule 7.

(2) Every e-PPI issuer shall contractually require merchants handling any authentication data to have security measures in place to protect such data.

(3) Every e-PPI issuer shall ensure that delivery of any software or initial authentication-related information, such as passwords or PINs, shall be carried out in a secure manner.

9. **Access to personal information.—**(1) The information referred to in Rule 7 shall not be disclosed to any person without the consent of the customer to whom it relates.

(2) Access to confidential information by the employees of the e-PPI issuer shall be on a "need-to-know" and "need-to-use" basis. The process of maintaining confidentiality of information shall be included in the information security policy.

10. **Reasonable security practices to be applicable.—**The financial data of the customer shall be deemed to be sensitive personal data or information for the purposes of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and every e-PPI issuer shall maintain and implement the practices and procedures prescribed in those rules.

11. **End-to-end encryption.—**Every e-PPI issuer shall ensure that end-to-end encryption is applied to safeguard the data exchanged, in accordance with the standards as may be prescribed by the Central Government under Rule 17.

12. **Traceability.—**Every e-PPI issuer shall have adequate processes in place to ensure that all interactions with customers or other service providers in relation to accessing payment accounts or initiating payments can be appropriately traced.

13. **Retention of information**.—Every e-PPI issuer shall retain data relating to electronic payments only for such period as may be specified by the Central Government.

14. **Reporting of cyber incidents**.—(1) Every e-PPI issuer shall establish a mechanism for monitoring, handling and follow-up of cyber incidents, cyber security incidents and cyber security breaches.

(2) CERT-In shall notify the categories of incidents and breaches that are required to be reported to it mandatorily. On the occurrence of such incident or breach, the e-PPI issuer shall report to CERT-In, the occurrence along with a report containing the measures taken to mitigate the impact.

(3) CERT-In may require e-PPI issuers to notify customers of cyber security incidents or breaches if the incident or breach is likely to result in harm to the customers.

15. **Customer awareness and education**.—(1) E-PPI issuers shall assist customers with regard to secure use of prepaid payment instruments.

(2) E-PPI issuers shall provide customer with all requisite information relating to security of prepaid payment instruments, including the following information:

(a) any equipment or software required by customers to access the prepaid payment instrument securely;

(b) the necessity of keeping passwords confidential and the manner in which these can be kept secure;

(c) procedure to be followed while accessing their payment account or initiating a payment;

(d) procedure to be followed in case of loss or theft of authentication data or if any fraud or abuse is detected;

(e) responsibilities of the e-PPI issuer and the procedure for grievance redressal.

(3) E-PPI issuers shall provide customers confirmation regarding initiation of payment to enable customers to check that the payment has been correctly initiated.

(4) E-PPI issuers shall keep customers informed of security procedures and of any new risks associated with the use of prepaid payment instruments.

(5) E-PPI issuers shall have in place a mechanism for customers to obtain assistance relating to their questions and complaints regarding use of prepaid payment instruments.

16. **Grievance redressal.—**Every e-PPI issuer shall designate a Grievance Officer for receiving complaints from customers..

(2) The e-PPI issuer shall publish on its website and its mobile application the name and contact details of the Grievance Officer, and procedure by which customers or any other person who suffers as a result of violation of these rules can make complaints to the Grievance Officer.

(3) The Grievance Officer shall act within 36 hours and shall resolve the complaint within one month from the date of receipt of such complaint.

17. **Security standards**.—(1) The Central Government may, by notification, specify the security standards to be adopted by e-PPI issuers for compliance with any or all these rules.

(2) If no standards are specified, the Central Government may make any other security standards applicable to e-PPI issuers for security of the payment systems operated by them.