GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.3457
TO BE ANSWERED ON 08.08.2018

LEGAL STEPS TO GUARD DIGITAL PAYMENTS

3457 SHRI BHAGWANTH KHUBA:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether the Government is taking any legal steps to guard digital payments;
(b) if so, the details thereof;
(c) whether the Government has appointed any committee for monitoring of measures for safety of digital payment; and
(d) if so, the details thereof;
(e) whether any complaints have been registered in their regard so far;
(f) if so, the details thereof?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S. S. AHLUWALIA)

(a) and(b): Yes, Sir. Some of the steps taken by Government to guard the digital payments are mentioned in Annexure 1. In addition, the steps taken by RBI to guard the digital payments are mentioned in Annexure 2.

(c) and (d): As per the information received from Ministry of Home Affairs, an Inter-Ministerial Committee on Phone Frauds has been constituted under the Ministry of Home Affairs which is periodically reviewing various aspects of dealing with phone frauds in pursuance of these reviews, FCORD-FICN Coordination Agency of Intelligence Bureau has been designated as central Nodal Agency to coordinate with States / UTs for facilitating investigations. In this connection MHA vide letter dated 12th February, 2018 has issued an advisory to all States / /UTs.

(e) and (f): Do not arise.

****

ANNEXURE-I

In addition, steps taken by Government to secure digital payment system are as under:

1. Government has formulated Cyber Crisis Management Plan for countering cyber-attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
2. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities along with countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 27 advisories have been issued for users and institutions.
3. CERT-In has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.
4. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.
5. Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In where organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.
6. Cyber security awareness sessions are conducted by Ministry of Electronics and Information technology (MeitY) under the Digishala Awareness Campaign.
7. Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.
8. Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance;

9. CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including CISOs of Government and critical sector organisations to give an exposure on current threat landscape and countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

******

ANNEXURE-II

Some of the measures taken by RBI are as follows-

1. A comprehensive circular on Cyber Security Framework in Banks issued on June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16), includes section on **'Arrangement for continuous surveillance'** in banks and also covers best practices pertaining to various aspects of cyber security

2. RBI has also set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond. Based on market intelligence and incidents reported by the banks, advisories are issued to the banks for sensitizing them about various threats and ensure prompt preventive/corrective action.

3. Department of Banking Supervision under RBI, with the help of Indian – Computer Emergency Response Team (CERT-In), conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios.

4. RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. Banks have also been following the same with their users.

5. RBI has set up a Cyber Security and IT Examination (CSITE) cell in 2015 and carries out Information Technology (IT) Examination of banks separately from the regular financial examination of the banks to assess their cyber resilience. The examination, inter-alia, evaluates the processes implemented by banks for security checks like Vulnerability Assessment (VA) / Penetration Testing (PT) etc. and their follow up action.

6. An inter-disciplinary Standing Committee on Cyber Security at RBI, reviews the threats inherent in the existing/emerging technology and suggests appropriate policy interventions to strengthen cyber security and resilience.

7. RBI has set up an Information Technology (IT) Subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.

8. Banks and Payment System Operators have been advised to enhance the security and risk mitigation measures for (a) card transactions (includes card based online transactions) and (b) electronic payment transactions (includes e-banking transactions) by taking following measures:-

a) Banks have been advised to provide **online alerts** for all card transactions (card present and card not present), vide, RBI circular dated February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and March 29, 2011 (DPSS. CO. PD 2224 /02.14.003/2010-2011).

b) Banks have been advised, vide, circular February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and December 31, 2010 (DPSS.CO.No.1503/02.14.003/2010-2011) to put in place a system of providing **additional factor of authentication** (2FA) for all card not present transactions using the information which is not available on the card.

c) Banks have also been advised vide circulars dated February 28, 2013 (DPSS (CO) PD No.1462 / 02.14.003 / 2012-13) and June 24, 2013 (DPSS (CO) PD No.2377 / 02.14.003 / 2012-13) for securing electronic (online and e-banking) transactions, to introduce **additional security measures**.

9. For Non-Bank Entities operating Payment Systems in India, in order to ensure that the technology deployed to operate the payment system/s authorised is/are being operated in a safe, secure, sound and efficient manner, RBI has, vide circulars DPSS.AD.No.1206 / 02.27.005 / 2009-2010 dated December 7, 2009 and DPSS.1444/ 06.11.001/ 2010-2011 dated December 27, 2010, which was subsequently amended vide circular DPSS.CO.OSD.No.2374 / 06.11.001 / 2010-2011 dated April 15, 2011 (copy is available on https: // www .rbi. org. in/ scripts/ FS_Notification .aspx?Id =6344&fn=9&Mode=0), mandated System Audit to be done on an annual basis by Certified Information Systems Auditor (CISA), registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI). Further, the scope of the System Audit should include evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc. The audit should also comment on the deviations, if any, in the processes followed from the process flow submitted to the Reserve Bank while seeking authorization.

10. With a view to address the issue of cyber resilience, RBI had, vide circular DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 9, 2016 (copy is available on https :// www. rbi.org.in / scripts / FS_Notification.aspx ?Id =10772&fn =9&Mode=0), instructed all authorised entities/ banks issuing PPIs in the country to carry out special audit by empanelled CERT-In auditors and take appropriate measures on mitigating phishing attacks.

In addition, details of direction pertaining to security for PPI transactions, are available in section 'Security, Fraud prevention and Risk Management Framework' of the Master Directions for PPI issued by RBI (DPSS.CO.PD.No.1164/02.14.006/2017-18).

11. RBI has issued various circulars wherein customer banks are advised to educate customers. These circulars are as follows:
    a) Card Payments – Relaxation in requirement of Additional Factor of Authentication for small value card present transactions dated May 14, 2015 (DPSS.CO.PD.No.2163/02.14.003/2014-2015).
    b) Cash Withdrawal at Point-of-Sale (POS) - Enhanced limit at Tier III to VI Centres dated August 27, 2015 (DPSS.CO.PD.No.449/02.14.003/2015-16).
    c) Card Not Present transactions –Relaxation in Additional Factor of Authentication for payments upto 2000/- for card network provided authentication solutions dated December 6, 2016 (DPSS.CO.PDNo.1431/02.14.003/2016-17).
    d) Master Direction on Issuance and Operation of Prepaid Payment Instruments dated October 11, 2017 (DPSS.CO.PD.No.1164/02.14.006/2017-18).
    e) Banks have also been requested to educate customers about cyber security risks, as per the circular on Cyber Security Framework in Banks dated June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16).

****