GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 4092
TO BE ANSWERED ON: 07.04.2017

INCREASE IN CYBER CRIMES RELATED TO E-TRANSACTIONS

4092. SHRI MOTILAL VORA:

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

(a) whether e-transaction related cyber crimes registered an increase of 73.24 per cent in the year 2015-16;
(b) whether an apprehension of 60 to 65 per cent increase in cases of cyber fraud has been raised in a joint study titled "Strategic National Measures to Combat Cybercrime" by industry association, ASSOCHAM and research firm Ernst and Young;
(c) if so, arrangements being made by Government to check the spike in cyber crime and whether Government would make stringent laws for this; and
(d) the steps being taken by Government for providing speedy justice to victims of fraud in digital transactions?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a): As per the data made available by Reserve Bank of India (RBI), a total of 13083 and 16468 cases related to Cyber Frauds (ATM/ Debit Card, Credit Card & Net Banking frauds) were reported by the banks during the years 2014-15 and 2015-16 respectively showing a rising trend.

(b): Yes, Sir. A study report "Strategic National Measures to Combat Cybercrime" prepared by industry association ASSOCHAM and research firm Ernst & Young has predicted an increase of 60 to 65 per cent in cases of cyber fraud in the year 2017.

(c): With the increase in digitization, the cyber attacks are also growing worldwide. Strengthening of cyber security is a continuing process. It is the primary responsibility of agencies involved in online payment to maintain adequate cyber security of their payment systems to avoid any mishap. Besides, Government has taken several steps towards enabling a secure online payment system. Some of the steps taken in this regards are as follows:

(i) RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

(ii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities alongwith countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 21 advisories have been issued for users and institutions.

(iii) In addition, all authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by Indian Computer Emergency Response Team (CERT-In) through the Reserve Bank of India to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

(iv) All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

(v) Further, Actions have been initiated by the Government to set up Financial CERT to handle cyber security incidents relating to Financial Sector.

(vi) Reserve Bank of India (RBI) carries out IT Examination of banks separately from the regular financial examination of banks from last year. This examination report has a special focus on cyber security. The examination reports have been issued to the banks for remedial action.

(i) RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from such incidents.

(ii) Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.

(iii) RBI also has set up an IT subsidiary, which would focus inter-alia on cyber security within RBI as well as in regulated entities. The subsidiary is in the process of recruiting the experts.

(iv) RBI has issued circular on 9th December 2016 on Security and Risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instruments (PPI) in the country.

(v) In addition, RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

(vi) RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.

(d): RBI, while giving certification of authorisation to non-bank entities for issuance and operation of PPIs, insists, in one of the term & conditions imposed on the entity, to put in place a proper customer grievance redressal mechanism. The entity is required to provide a window for 16 x 7 (16 hours - 7 days) to enable the customer or system participant for lodging the complaints. Further, the entity is also required to display the name(s) and contact details of its nodal officer(s) including phone numbers for customer service along with the grievance redressal mechanism on its website including the minimum definite time frame for resolution of complaints.

RBI has issued Master Circular – 'Policy Guidelines on Issuance & Operation of Pre-paid Payment Instruments in India'. In cases where the customer files a complaint with the bank disputing a transaction, it would be the responsibility of the service providing bank, to expeditiously redress the complaint. Customers' complaints / grievances arising out of mobile banking facility would be covered under the Banking Ombudsman Scheme.

****