

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**RAJYA SABHA**  
**STARRED QUESTION NO. \*65**  
TO BE ANSWERED ON: 21-07-2017

**CASES OF FRAUD IN DIGITAL PAYMENTS**

**\*65      SHRI NARESH AGRAWAL:**

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

- (a) whether it is a fact that the number of cases of fraud in digital payments have increased, if so, the reasons therefor;
- (b) the steps taken by Government in respect of digital security; and
- (c) the suggestions made by Chandra Babu Naidu Committee on digital security?

**ANSWER**

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY  
(SHRI RAVI SHANKAR PRASAD)

(a) to (c):    A Statement is laid on the Table of the House.

**STATEMENT REFERED TO IN REPLY TO RAJYA SABHA STARRED QUESTION \*65 FOR 21-07-2017  
REGARDING CASES OF FRAUD IN DIGITAL PAYMENTS**

(a): The number of cases of frauds involving credit cards, ATM/Debit cards and Internet banking during the year 2015-16 and 2016-17 are as follows:

<u>2015-16</u>	<u>2016-17</u>
16468	13653

For prepaid payments instruments including e-wallets, Reserve Bank of India (RBI) has started maintaining provisional data of fraudulent transactions. According to the data for March, April and May 2017, the number of fraudulent transactions is between 0.005% to 0.007% of the total number of transactions.

As per incidents reported to the Indian Computer Emergency Response Team (CERT-In), 40 phishing incidents affecting 19 financial organisations and 10 incidents affecting ATMs, Point of Sales (POS) systems and Unified Payment Interface (UPI) have been reported during November 2016 to June 2017.

As part of promotion of digital payments, Government is taking several steps to ensure that frauds are minimised and even when an incident of this nature takes place, corrective action is immediately taken.

(b): The steps taken by Government to secure digital payment system are placed at Annexure.

(c): The Committee of Chief Ministers on Digital Payment, chaired by Chief Minister of Andhra Pradesh Shri Chandrababu Naidu, has in its Interim Report suggested the following on Digital Payment security:

- (i) The Standing Committee formed under Chairmanship of Secretary, MeitY and DoT should focus on strengthening NPCI security system, consultations with private service providers, banks and RBI.
- (ii) Government should come out with an insurance scheme to cover losses incurred in digital transactions on account of fraud, etc. In order to address the apprehension of general public in adopting digital payments. The scheme should target low ticket transactions to cover the vulnerable sections like small merchants, farmers etc.
- (iii) A separate Authority may be set up for Digital Payments. The Authority will be responsible for overseeing sector development, regulatory issues, security aspects, etc. Necessary legislative and policy changes may be effected to create this body.

**Annexure**

**Steps taken by Government to secure digital payment system**

1. 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, 25 advisories have been issued for users and institutions.
2. In addition, all authorised entities/banks issuing PPIs in the country have been advised by CERT-In through the Reserve Bank of India to carry out security audit by the empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.
3. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.
4. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 15 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 148 organizations from different sectors including Finance sector.
5. Cyber security awareness sessions are conducted by Ministry of Electronics and Information technology (MeitY) under the Digishala Awareness Campaign.
6. 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.
7. MeitY has organised 2 workshops for banks, Internet Service Providers (ISPs) and Prepaid Payment Instruments (PPIs) issuing entities regarding security of digital payments systems.
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
10. RBI has set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.
11. Department of Banking Supervision under RBI, with the help of CERT-In, conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios.
12. RBI has issued a circular on 9<sup>th</sup> December 2016 for security and risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

13. 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.
14. RBI has set up a Cyber Security and IT Examination (CSITE) cell in 2015.
15. 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.
16. RBI has prepared draft Master Directions on issuance and operations of prepaid payments instruments in India and on 20 March 2017 has invited public comments on the same.

\*\*\*\*\*