GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2759
TO BE ANSWERED ON 10.07.2019

SAFETY AND SECURITY OF DIGITAL TRANSACTIONS

2759 SHRI PARVESH SAHIB SINGH:

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

(a) whether the Government has taken note of RBI report predicting rise of digital transactions by four times by 2021 and if so, the details thereof and the reaction of the Government thereto;
(b) whether the Government is taking steps to strengthen safety and security of digital transactions to prevent online frauds and if so, the details thereof;
(c) whether there is any existing separate laws for regulation and governance of mobile wallets and all other facilitator of digital financial transactions and if so, the details thereof; and
(d) if not, whether the Government proposes to enact any law in this regard??

ANSWER

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

(a): This Ministry is aware of the surge in digital transactions. Government is taking various initiatives to further increase the digital payments transactions. Government has presented its view/recommendation report to RBI committee on "Deepening of Digital Payments". Government has taken a note of the RBI report-predicting rise in digital transactions by four times by 2021.
As per, RBI Payment and Settlement Systems in India: Vision – 2019-2021, payment systems like UPI / IMPS are likely to register average annual growth of over 100% and NEFT at 40% over the vision period. The number of digital transactions is expected to increase more than four times from 2069 crore in December 2018 to 8707 crore in December 2021. More data on growth has been presented in Annexure I.

(b): The steps taken by Government to create awareness as well as further strengthen the security system and legal framework have been mentioned in Annexure II. In addition, the steps taken by Reserve Bank of India (RBI) in respect of digital payments security have been mentioned in Annexure III.

(c): There are no existing separate laws for regulation and governance of mobile wallet and all other facilitator of digital financial transaction. However, the Reserve Bank of India (RBI) had issued 'Master Direction on Issuance and Operation of PPIs' (MD on PPIs) (DPSS.CO. PD. No.1164/02.14.006/2017-18) dated October 11, 2017 (updated as on February 25, 2019).
(d): No, Sir.

Annexure-I

Please find below the data on growth of digital payments for the past three years.

Year	2016-17	2017-18	2018-19
Transaction volume (in cr)	1004	2017	3134

data source : published by MeitY

The total transaction volume for the year FY18-19 was 3134 cr, with a growth rate of 55% over last year. The government is well poised to attain the ambitious target of 4000cr digital transaction for FY19-20.

*****

Annexure -II

Initiatives by the Government of India

In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners and users to protect networks and data by way of hardening and deploying appropriate security controls.

1. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies.
2. All authorised entities/ banks issuing PPIs in the country have been advised by CERT-In through Reserve bank of India to carry out special audit by 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. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
4. Government has empanelled security auditingorganizations to support and audit implementation of Information Security Best Practices.
5. All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
6. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
7. Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeSect participated.
8. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.
9. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.
10. Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.
11. Under the Information Security Education and Awareness (ISEA) Project, candidates are trained in various formal/non-formal courses in Information Security.

Annexure-III

Steps taken by RBI

Department of Payment and Settlement Systems (DPSS), Reserve Bank of India (RBI) has issued circulars/ guidelines related to security and risk mitigation measures for securing digital / online payment transactions.

1. Securing Card Transactions

Various measures have been taken by RBI to secure card transactions and issued advisories: -

i) Banks have been advised to provide online alerts for all card transactions {Card Present (CP) and Card Not Present (CNP)}, vide, RBI circular dated March 29, 2011.

ii) RBI has also issued circulars dated September 22, 2011, February 28, 2013 and June 24, 2013 for securing electronic (online and e-banking) transactions advising banks to introduce additional security measures, as follows:
   a) All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customers. Such cards enabling international usage will have to essentially be EMV Chip and PIN enabled.
   b) Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their card internationally atleast once (for/ through e–commerce/ATM/POS).
   c) Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry-Data Security Standards) and PA-DSS (Payment Applications-Data Security Standards).
   d) Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants.

iii) RBI has directed banks to mandatorily put in place an Additional Factor of Authentication (AFA) for all CNP transactions w.e.f. 01.05.2013 failing which the issuer bank shall reimburse the loss to customer without demur.

iv) All authorised card payment networks are permitted to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to certain conditions. All extant instructions of RBI on safety and security of card transactions, Including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also (DPSS.CO.PD No.1463/02.14.003/2018-19) dated January 08, 2019).

v) The systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions.

2. Securing Payments through Internet Banking / Electronic Payments

RBI has issued circular on 'Security and Risk Mitigation Measures for Electronic Payment Transactions' (DPSS.CO.PD No.1462 /02.14.003 /2012-13) dated February 28, 2013. Vide this circular, RBI has required banks to introduce following additional measures to secure electronic mode of payments like RTGS, NEFT and IMPS.

3. Prepaid Payment Instruments (PPIs):

RBI has issued 'Master Direction on Issuance and Operation of PPIs' (MD on PPIs) (DPSS.CO. PD. No.1164/02.14.006/2017-18) dated October 11, 2017 (updated as on December 29, 2017).

4. Limiting Customer Liability on Unauthorized Electronic Banking Transactions

RBI has issued circular no. DBR.No. Leg.BC.78/09.07.005/2017-18 dated July 06, 2017 limiting the liability of customers on unauthorized electronic banking transactions.

5. Limiting Customer Liability in Unauthorized Electronic Banking Transactions in PPIs issued by Authorised Non-banks

RBI has issued circular no. DPSS.CO.PD.No.1417/02.14.006/2018-19 dated January 04, 2019 limiting the liability of customers in unauthorized electronic banking transactions in PPIs issued by Authorised Non-banks.

****