GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4793
TO BE ANSWERED ON 24.03.2021

DIGITAL FINANCIAL TRANSACTION

4793 SHRI RAHUL RAMESH SHEWALE:
SHRI HEMANT SRIRAM PATIL:
SHRI OMPRAKASH BHUPAL SINH ALIAS PAWAN RAJENIMBALKAR:

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

(a) whether the online frauds have increased in the country along with rise of digital financial transactions in the country;
(b) if so, the details thereof and the reasons therefor along with the reaction of the Government thereto;
(c) whether the Government has assessed the existing laws enacted for regulation and governance of digital financial transactions in the country;
(d) if so, the details and the outcome thereof and if not, the reasons therefor; and
(e) the other steps taken/being taken by the Government to make digital financial transactions safe in the country along with achievements thereof?

ANSWER

MINISTER OF STATE ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): Online or Digital payments have been on a rise especially after the spread of COVID19 pandemic in the country. Based on the fraud reporting done by Banks, it is observed that frauds in online banking are primarily on account of Social engineering techniques like Vishing and Phishing. RBI has mandated two factor authentication which provides an additional layer of security to the end customers using online modes of payment. Additionally, customer awareness messages/campaigns are available on all prominent bank sites covering caution to be exercised by customers while performing online transactions.

(c) and (d): Government has taken policy level initiatives to ensure appropriate and secure functioning of digital payment transactions, in the country. As per RBI’s circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions dated July 6, 2017, customer’s entitlement to zero liability shall arise where the unauthorised transaction occurs in the events contributory fraud/ negligence/ deficiency on the part of the bank or third party breach where the deficiency lies neither with the bank nor with the customer, but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorisedtransaction. Further, RBI has introduced ‘Ombudsman Scheme for Digital Transactions, 2019’ in the public interest and in the interest of fair conduct of business relating to payment systems, to provide a mechanism of Ombudsman for redressal of complaints against deficiency in services related to digital transactions.

(e): Steps taken by the Government to make digital financial transactions safe in the country are provided in Annexure I.

****

Annexure I

Steps taken to enhance the security of digital payment transactions

Government has taken various steps to enhance the security of digital payment transactions in the country, as mentioned below:

1. RBI vide circular on Cyber Security Framework in Banks dated June 2, 2016, advised banks to, *inter alia*, implement as under:
   - Improve and maintain customer awareness and education with regard to cybersecurity risks.
   - Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.
   - Educate the customers on the downside risk of sharing their login credentials / passwords etc. to any third-party vendor and the consequences thereof.

2. RBI vide circular on "Control measures for ATMs – Timeline for compliance" dated June 21, 2018, advised banks and white label ATM operators to take various measures to strengthen security of ATMs. These measures, inter alia include - enabling BIOS passwords, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, implementing anti-skimming and whitelisting solution, upgrading ATMs to supported versions of operating system, etc.

3. RBI vide its circular on 'Enhancing Security of Card Transactions' dated 15.01.2020, has inter-alia issued following guidelines to banks, card payment networks and non-bank PPI issuers:
   - All the cards (physical/virtual) at the time of issue/re-issue are to be enabled for use only at contact based points of usage within India.
   - Facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc. on 24x7 basis to be provided.
   - Alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card to be provided.

4. RBI vide Master Direction on Digital Payment Security Controls dated February 18, 2021, advised banks to, *inter alia*, implement the following customer protection controls for their digital payment applications:
   - Incorporate secure, safe and responsible usage guidelines and training materials for end users within the digital payment applications.
   - Mention/ Incorporate a section on the digital payment application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge consumer grievances
   - Continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same, and caution the customers against

commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.

5. Banks to provide customers with 24x7 access through multiple channels (at a minimum via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and/ or loss or theft of payment instrument, such as, card, etc.

6. Banks have been directed to examine the fraud cases and report them to law enforcement agencies, examine staff accountability, complete proceedings against the erring staff expeditiously, take steps to recover the amount involved in the fraud, claim insurance wherever applicable and streamline the system as also the procedures so that frauds do not recur.

7. The customers will have zero liability in case of unauthorised transactions occurring due to contributory fraud / negligence / deficiency on the part of the bank and due to third party breach, provided, they notify the bank regarding the unauthorised transactions within three working days of receiving the communication from the bank regarding this transaction.

8. RBI is running the awareness campaign under the banner of 'RBI KehtaHai' on safe digital banking which inter-alia include:

- Not to share password /pin/OTP received through SMS.
- Act swiftly on alerts received on transactions, which customer have not initiated or not authorized.
- Practicing safe mobile banking, such as awareness on benefits of registering mobile number with bank for instant alerts.
- Not storing important banking data in mobile.
- Use only verified, secure and trusted website.
- Avoid banking transactions on free networks,
- Change PIN regularly.
- Blocking ATM card, Credit Card and prepaid card immediately if it is lost or stolen.

9. Ministry of Electronics & Information Technology (MEITY) is conducting programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "www.infosecawareness.in", and "www.cyberswachhtakendra.gov.in".

10. CERT-In is working in coordination with Reserve Bank of India (RBI) and Banks to track and disable phishing websites.

11. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. Regarding securing digital payments, 37 advisories have been issued for users and institutions.

12. Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

13. All authorised entities/ banks issuing prepaid payment instruments (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.

14. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

15. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 50 such drills have so far been conducted by CERT-In where 450 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. Out of these drills, 12 drills were conducted in coordination with the Reserve Bank of India and The Institute for Development and Research in Banking Technology for financial sector organisations.

16. Government is operating 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 for citizens and organisations.

****