GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2621
TO BE ANSWERED ON 10.03.2021

BANKING FRAUDS

2621 DR. KRISHNA PAL SINGH YADAV:

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

(a) whether the Government is aware about the increasing incidents of hacking of online banking and ATM card details and if so, the details thereof and the steps taken/being taken by the Government to check such incidents;
(b) whether the Government proposes to bring in new technology to check aforesaid incidents of online fraud and if so, the details thereof;
(c) whether the Government is aware about incidents of fraud by cloning of ATM card and if so, the details thereof and the steps being taken by the Government in this regard;
(d) whether the Government proposes to develop such technology which can track the card cloning process and alert the customers and if so, the details thereof; and
(a) the steps taken/being taken by the Government to check the increasing cases of fraud by obtaining OTP and other bank account details on phone calls?

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

(a) and (c): Steps are being taken by RBI, NPCI and Banks to prevent online banking frauds conducted primarily through Social engineering techniques like Phishing, and ATM card skimming. The detailed steps taken by the Government to enhance the security of online / digital transactions, including card transactions, and to check and control frauds are given in Annexure I. RBI has mandated the usage of EMV chip cards to address the problem of ATM card skimming. Customer awareness initiatives have been taken by RBI, NPCI and Banks regarding caution to be exercised by customers while performing online transactions.

(b): Banks constantly upgrade their IT infrastructure to ensure the security of digital payment transactions. Banks implement robust monitoring system to ensure that anomalies are triggered and customers are alerted for any suspicious behavior observed in their account. NPCI has adopted a layered approach of Prevent, Detect & Respond towards addressing Cyber Threats. Many banks have also deployed AI/ML based solutions to safeguard the interest of their customers. Further, RBI vide circular DoS.CO.CSITE.SEC.No. 1852/31.01.015/2020-21 dated February 18, 2021has issued directions regarding 'Digital Payment Security Controls' to Banks to ensure a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

(d): As of date, EMV chip on a card cannot be cloned making it a secure mode of transaction and has been mandated by RBI. Additionally, an SMS notification is mandatorily sent to the cardholders intimating them of the transaction carried out on their cards.

(e): Customer awareness campaigns carried out by ecosystem players educate customers that OTP is not supposed to be shared with third party. Additionally, it is also publicised that customers should not share any banking credentials to third party over a phone call.

****

Annexure I

Steps taken to enhance the security of digital payment transactions

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

Steps taken by CERT-In

a) 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.
b) 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 empaneled 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.
c) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
d) All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.
e) Government has empaneled 90 security auditing organizations to support and audit implementation of Information Security Best Practices.
f) 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.
g) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organizations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc. participated. Out of these drills, 11 drills were conducted in coordination with the Reserve Bank of India and The Institute for Development and Research in Banking Technology for financial sector organizations.
h) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organizations regarding securing the IT infrastructure and mitigating cyberattacks.
i) 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.
j) 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”.

Steps taken by Reserve Bank of India (RBI)

Following are the various steps taken by the Reserve Bank of India (RBI) to enhance security of online / digital transactions, including card transactions, and to check and control frauds; these also include various benefits (in terms of increased safety of transaction, efficiency in grievance redressal mechanism, etc.) being provided to customers:

1. In terms of instructions contained in circulars RBI / DPSS No. 1501 / 02.14.003 / 2008-2009 dated February 18, 2009, RBI / DPSS No. 2303 / 02.14.003 / 2009-2010 dated April 23, 2010, DPSS.CO.No.1503 / 02.14.003 / 2010-2011 dated December 31, 2010 and DPSS.PD.CO. No.223 / 02.14.003 / 2011-2012 dated August 04, 2011,
   a) It is mandatory to put in place a system of providing for additional authentication / validation based on information not visible on the cards for all on-line card not present transactions.
   b) In case of customer complaint regarding issues, if any, arising out of transactions effected without the additional factor of authentication, the issuer bank shall reimburse the loss to the customer further without demur.

2. In terms of RBI / DPSS No.914 / 02.14.003 / 2010-2011 dated October 25, 2010 and DPSS.PD.CO. No.371 / 02.14.003 / 2014-2015 dated August 22, 2014,
   a) The mandate for additional authentication / validation shall apply to all transactions using cards issued in India, for payments on merchant site where no outflow of foreign exchange is contemplated. The linkage to an overseas website/payment gateway cannot be the basis for permitting relaxations from implementing the mandate. The mandate is not presently applicable for use of cards issued outside India, on Indian merchant sites.
   b) Where cards issued by banks in India are used for making card not present payments towards purchase of goods and services provided within the country, the acquisition of such transactions has to be through a bank in India and the transaction should necessarily settle only in Indian currency, in adherence to extant instructions on security of card payments.
3. As per RBI Master Direction DPSS.CO.PD.No.1164 / 02.14.006 / 2017-18 dated October 11, 2017 (as updated from time to time) on “Issuance and Operation of Prepaid Payment Instruments (PPIs)”,
   a) Issuers shall introduce a system where every successive payment transactions in wallet is authenticated by explicit customer consent.
   b) Cards (physical or virtual) shall necessarily have AFA as required for debit cards, except in case of PPIs issued under PPI-Mass Transit Systems (PPI-MTS).
4. For better customer protection, card networks have been advised to ensure the following for all face-to-face / Card Present (CP) transactions performed using cards issued and acquired by banks in India:
   a) Mandatory PIN authentication for all transactions performed using credit, debit and prepaid cards – magnetic stripe or EMV Chip and PIN based. Issuer banks to accordingly comply with this requirement.
   b) While processing and EMV Chip and PIN card, fall back to magnetic stripe option shall be enabled only if the transaction cannot be completed as a Chip based transaction, i.e. *ab initio* processing of EMV Chip and PIN based cards on the basis of magnetic stripe data shall not be done. Further, specific code for all such fall back transactions shall be indicated in the transaction message sent to the issuer.
   c) Acquirer banks shall be liable for any loss to customers in case of failure to ensure adherence to contents of para 4 (b) above.
   d) Instructions at para 4 (a) above will not affect provisions of RBI circulars cited below at para 5.

5. In terms of RBI circulars DPSS.CO.PD.No.2163/02.14.003/2014-2015 dated May 14, 2015 and DPSS.CO.PD No.752/02.14.003/2020-21 dated December 04, 2020, Additional Factor of Authentication (AFA) requirement has been relaxed for values up to Rs. 5,000/- per transaction for card transactions in contactless mode at Point of Sale (PoS) terminals performed using NFC-enabled EMV Chip cards. Transactions beyond this limit can be processed in contactless mode, but with AFA.
6. In terms of RBI circulars DPSS.CO.PD No.1421/02.14.003/2016-17 dated December 02, 2016 and DPSS.CO.PD No.892/02.14.003/2016-17 dated September 29, 2016, all new card present acceptance infrastructure deployed with effect from July 1, 2017 are enabled for processing payment transactions using Aadhaar-based biometric authentication also. As regards enablement of existing card acceptance infrastructure for processing payment transactions using Aadhaar-based biometric authentication, the timeline will be advised in due course.
7. In terms of RBI circular DPSS. CO. PD 2224/02.14.003/2010-2011 dated March 29, 2011, banks may put in place a system of online alerts for all types of transactions irrespective of the amount, involving usage of cards at various channels.
8. In terms of RBI circular DPSS (CO) PD No.1462/02.14.003 / 2012-13 dated February 28, 2013, banks should frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorised card payment networks for arresting fraud. Banks should build in a system of call referral in co-ordination with the card payment networks based on these rules. Further, all new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer.

   The above circular also prescribes certain safety measures for electronic payment modes like RTGS, NEFT and IMPS. These inter alia include a system of alert may be introduced when a beneficiary is added; limit on the number of beneficiaries that may be added in a day per account could be considered; introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered; etc.

9. As per RBI circular DPSS.CO.PDNo.1431/02.14.003/2016-17 dated December 6, 2016, the AFA requirement for transactions upto Rs.2,000/- for online CNP transactions for the 'payment authentication solutions' provided by authorised card networks with the participation of respective card issuing and acquiring banks has been relaxed, subject to conditions specified in the circular.
10. Vide circular DPSS.CO.PD No.1463/02.14.003/2018-19 dated January 08, 2019, RBI has permitted authorised card payment networks to offer card tokenisation services to any token requestor, subject to the conditions listed in the circular. This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.). All extant instructions of the 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. The ultimate responsibility for the card tokenisation services rendered rests with the authorised card networks.
11. Vide circulars DPSS.CO.PD.No.447 / 02.14.003 / 2019-20 dated August 21, 2019 and DPSS.CO.PD No.754 / 02.14.003 / 2020-21 dated December 04, 2020, the RBI has permitted processing of e-mandate on cards for recurring transactions (merchant payments) with AFA during e-mandate registration, modification and revocation, as also for the first transaction, and simple / automatic subsequent successive transactions, subject to conditions listed in the circular. This circular is applicable for transactions performed using all types of cards – debit, credit and Prepaid Payment Instruments (PPIs), including wallets. The maximum permissible limit for a transaction under this arrangement shall be Rs.5,000/-. The scope of this arrangement has been extended to cover UPI transactions as well. Further, processing of recurring transactions (domestic or cross-

border) using cards / PPIs / UPI under arrangements / practices not compliant with the aforesaid instructions shall not be continued beyond March 31, 2021.

12. Following are in terms of circular DPSS.CO.PD No.1343/02.14.003/2019-20 dated January 15, 2020
    a) At the time of issue / re-issue, all cards (physical and virtual) shall be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Issuers shall provide cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions, as per the process outlined below.
    b) Additionally, the issuers shall provide to all cardholders:
        i. 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.;
        ii. the above facility on a 24x7 basis through multiple channels - mobile application / internet banking / ATMs / Interactive Voice Response (IVR); this may also be offered at branches / offices;
        iii. alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card.
    c) The provisions of this circular are not mandatory for prepaid gift cards and those used at mass transit systems.
13. In terms of circular DPSS.CO.PD.No.1810 / 02.14.008 / 2019-20 dated March 17, 2020, Payment Aggregators (PAs) shall not give an option for ATM PIN as a factor of authentication for CNP / online transactions. PAs shall not store the customer card credentials within their database or the server accessed by the merchant.
14. All new cards issued – debit and credit, domestic and international – by banks shall be EMV chip and PIN based cards.
15. In terms of RBI circular DPSS.CO.PD.No.808/02.14.006/2018-19 dated October 16, 2018, banks shall ensure that all new PPIs issued in the form of cards are EMV Chip and PIN compliant. Banks shall also ensure that all reissuance / renewal of PPIs in the form of cards are EMV Chip and PIN compliant. As non-bank PPI issuers are issuing interoperable cards in association with card networks for the first time, the cards issued by these entities shall ab initio be EMV Chip and PIN compliant. PPI issuers operating exclusively in Meal segment shall issue EMV Chip and PIN compliant cards, if they opt for interoperability. Gift cards and MTS, may however, be issued with or without EMV Chip and PIN enablement.
16. RBI has issued instructions to limit the liability of customers in case of unauthorised electronic transactions. Additionally, a customer may lodge his / her grievance under the Banking Ombudsman (BO) Scheme / Ombudsman Scheme for Digital Transactions of RBI.
17. Vide RBI circular DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019, instructions have been issued to all operators and participants of authorised payment systems, for time-bound resolution of failed transactions; failure to do so may lead to payment of compensation – *as prescribed in the circular* - to customers.
18. In terms of RBI circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020, authorised Payment System Operators (PSOs) – banks and non-banks – and their participants have been advised to put in place system/s for Online Dispute Resolution (ODR) system for resolving disputes and grievances of customers. To begin with, authorised PSOs shall be required to implement an ODR system for disputes and grievances related to failed transactions in their respective payment systems.
19. For increasing customer awareness about safe banking, RBI has been running campaigns in media / social media under the “RBI KehtaHai” initiative.
20. To prevent fraudulent withdrawal at ATMs, RBI had mandated, vide circular DPSS. CO.PD.No. 289/02.10.002/2013-2014 dated August 1, 2013, requirement of PIN entry for each and every

transaction, including balance enquiry transactions. As an additional safety measure, it was advised that the time out sessions should be enabled for all screens / stages of ATM transaction keeping in view the time required for such functions in normal course; banks may ensure that no time extensions are allowed beyond a reasonable limit at any stage of the transaction.

21. RBI circular DPSS.CO.PD.No./2895/02.10.002/2015-2016 dated May 26, 2016 advised banks and White Label ATM operators to ensure that all their ATMs / micro-ATMs (which are enabled to handle card-based payments) are enabled for EMV Chip based processing of transactions.
22. RBI circular DPSS.CO.PD.No.1198 / 02.14.006 / 2019-20 dated December 24, 2019 has inserted para 9.1 (iii) in the Master Direction on Issuance and Operation of PPIs dated October 11, 2017 (PPI-MD). This has introduced new type of semi-closed PPI to give impetus to small value digital payments and for enhanced user experience. Such PPIs shall be issued by bank and non-bank PPI issuers after obtaining minimum details of PPI holder and has the following features:
    a) These PPIs shall be reloadable in nature and issued in card or electronic form. Loading / reloading shall be from a bank account and / or credit card.
    b) The amount loaded in such PPIs during any month shall not exceed Rs. 10,000/- and the total amount loaded during the financial year shall not exceed Rs. 1,20,000/-.
    c) The amount outstanding at any point of time in such PPIs shall not exceed Rs. 10,000/-.
    d) These PPIs shall be used only for purchase of goods and services and not for funds transfer.

The RBI circulars cited above are available on RBI website at following path: https://www.rbi.org.in/Scripts/NotificationUser.aspx

23. Consequent upon announcement made by the Reserve Bank of India in the Statement on Developmental and Regulatory Policies of the Third Bi-monthly Monetary Policy Statement for 2019-20 dated August 07, 2019 for creation of a Central Payments Fraud Information Registry (CPFIR), a web-based fraud reporting solution has been implemented from March 23, 2020. All payment related frauds are reported through the Electronic Data Submission Portal (EDSP) of RBI.The reporting through the system is yet to be stabilised in terms of on-boarding of all banks and non-bank PPI Issuers. The Reserve Bank is also in the process of migrating this EDSP system to a comprehensive fraud reporting and monitoring platform to facilitate analysis of the prevalent frauds reported by banks and non-bank Prepaid Payment Instrument Issuers.
24. All Scheduled Commercial Banks and non-bank Prepaid Payment Instrument issuers are required to report payment related frauds in the portal. All payment related frauds undertaken using various payment instruments (bank account, credit card, debit card, paper-based instruments, PPIs) and processed through authorised payment systems are required to be reported by banks / non-bank entities in EDSP. The channel through which the payment frauds took place is also captured (internet, mobile, branch, Point of Sale (PoS) terminals, ATM, etc.) in the system. The frauds reported in EDSP by banks / non-bank entities are either reported by customers or detected by the entities themselves.

****