GOVERNMENT OF INDIA
MINISTRY OF FINANCE
LOK SABHA
UNSTARRED QUESTION NO- †3461
ANSWERED ON- 08/08/2022

CYBER CRIMES AND ONLINE FRAUDS

†3461. SHRI MOHANBHAI KALYANJI KUNDARIYA
SHRI ANIL FIROJIYA
SHRI SUMEDHANAND SARASWATI
SHRIMATI RANJEETA KOLI
DR. MANOJ RAJORIA
SHRI RAMSHIROMANI VERMA

Will the Minister of FINANCE be pleased to state:-

(a) whether the Government is aware of the incidents of cyber crimes by hacking details of online banking and ATM cards as well as through various new methods;

(b) if so, the details thereof including the number of cases registered for such frauds and the number of such cases settled so far;

(c) whether the Government proposes to introduce any new technique to curb the incidents of online frauds;

(d) if so, the details thereof; and

(e) the steps taken/proposed to be taken by the Government to check the increasing cases of frauds by obtaining bank account details through OTP and other modes on phone calls?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) to (e): As per Reserve Bank of India (RBI) data on frauds reported by Scheduled Commercial Banks (SCBs) under the category "Card/Internet- ATM/Debit Cards, Credit Cards and Internet Banking", the amount involved in such frauds, based on the year of occurrence, has declined from Rs. 185 crore in the financial year 2019-20 to Rs. 160 crore in the financial year 2020-21 {year-on-year (Y-o-Y) decline of 15.2%} and to Rs. 128 crore in the financial year 2021-22 (Y-o-Y decline of 17.5%).

As per information received from the National Crime Records Bureau regarding cases registered in respect of such frauds, the latest published data pertains to the year 2020, according to which, in respect of frauds related to ATMs/ credit cards / debit cards, online banking and OTP in the year 2020, 8494 cases were registered and 4103 cases were disposed of.

RBI has issued instructions on Cyber Security Framework in Banks and have mandated SCBs to report all unusual cyber incidents to RBI within two to six hours of occurrence of such incidents. These incidents are analysed for the pattern of attack and the vulnerabilities exploited, and where needed, advisories/alerts are issued to the banks so as to avoid repeat attacks/exploitation of the same vulnerabilities. Further, the incidents are also analysed from the point of view of

sophistication of attack as well as the systemic impact, and are categorised under critical, high, medium and low categories. RBI also reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. Comprehensive steps taken in order to strengthen security of digital transactions, *inter alia,* include the following:

(i) A comprehensive circular on Cyber Security Framework in Banks was issued by RBI on 2.6.2016, wherein banks were advised to put in place a board-approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.

(ii) Guidelines on Cyber Security Controls for third party ATM Switch Application Service Providers (ASPs) have been issued by RBI on 31.12.2019.

(iii) Master Directions on Digital Payment Security Controls have been issued by RBI on 18.2.2021, wherein banks have been advised to put in place necessary controls to protect the confidentiality and integrity of customer data, and processes associated with the digital product/services offered.

(iv) A National Cyber Crime Reporting Portal has been launched by the Ministry of Home Affairs to enable public to report incidents pertaining to all types of cybercrimes, and a toll-free number has also been operationalised to get assistance in lodging online complaints.

(v) For immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters, Financial Cyber Fraud Reporting and Management System module has been made operational by the Indian Cyber Crime Coordination Centre (I4C), working under the Ministry of Home Affairs.

(vi) The Indian Computer Emergency Response Team (CERT-IN) under the Ministry of Electronics and Information Technology issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies, and is working in coordination with service providers, regulators and LEAs to track and disable phishing websites and facilitate investigation of fraudulent activities.

In addition to this, a number of steps have been taken to enhance security of digital payment transactions, including those of card transactions, online transactions *etc.*, and to reduce online banking frauds which include, *inter alia*, the following –

(i) conversion of magnetic strip card to EMV chip and PIN cards;
(ii) mandating enablement of online alerts for all transactions;
(iii) certification of merchant terminals;
(iv) mandating PIN entry for all ATM transactions
(v) enabling all ATMs for processing EMV chip and PIN cards;
(vi) restricting international usage by default and enablement of the same only after specific mandate from the customer;
(vii) Capping the value/mode of transactions/beneficiaries;
(viii) setting daily limits; and
(ix) issuing alerts upon addition of beneficiaries.

Further, to spread awareness against cyber-crimes, several steps have been taken which include, *inter alia,* dissemination of messages on cyber-crime through short message service(SMS), radio campaigns, publicity on prevention of cyber-crime and cyber safety tips through social media accounts of the Indian Cybercrime Coordination Centre (I4C), publishing of a handbook for adolescents/students, publishing of Information Security Best practices for government officials, organising of cyber safety and security awareness weeks in association with States and Union territories, conducting of electronic-banking awareness and training (e-BAAT) programmes by RBI focussed, *inter alia* on awareness about frauds and risk mitigation.

*****