GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA

UNSTARRED QUESTION No. 2274

Answered on Monday, March 8, 2021/Phalguna 17, 1942 (Saka)

ATM Frauds

2274. SHRI RODMAL NAGAR:SHRI KANAKMAL KATARA:

Will the Minister of FINANCE be pleased to state:

(a) the steps being taken by the Government to check hacking of ATM card details keeping in view the rising number of such cases in the country;
(b) whether with a view to preventing ATM related or online fraud, the Government is developing any such technology so as to track cloning of the cards immediately and also to alert the account holders;
(c) if so, the details thereof and if not, the reasons therefor; and
(d) the details of the steps being taken by the Government to check the increasing number of cases of fraud after getting OTP and other secret information on phone in the various cities of the country including the National Capital Region?

Answer

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE
(SHRI ANURAG SINGH THAKUR)

(a) to (d) Reserve Bank of India (RBI) has issued circulars/guidelines from time to time, for preventing bank frauds and suitably protecting the interest of the customers which, inter-alia, includes:

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. RBI is running the awareness campaign under the banner of 'RBI Kehta Hai' 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.

****