

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3370
TO BE ANSWERED ON: 23.03.2022

ONLINE BANKING FRAUDS

3370. SHRIMATI GOMATI SAI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government is aware of the increasing incidents of online-banking frauds and hacking of the ATMs and data and if so, the details thereof along with the steps taken by the Government to check such incidents;
- (b) whether the Government proposes to bring in new technique to check the aforesaid incidents of online frauds and if so, the details thereof;
- (c) whether the Government is aware of the fraudulent activities like cloning of ATM cards and if so, the details thereof and the steps being taken by the Government in this regard; and
- (d) the details of the steps taken/being taken by the Government to check the rising cases of frauds by obtaining the OTP and other bank details on phone calls?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): Government of India is making focussed efforts on ensuring security of digital payments and creating awareness in citizens about secure digital payment practices. Online banking and ATM transactions are secured with two factor authentication for safety of the customers. Online-banking frauds are perpetrated primarily due to customer compromising credentials unknowingly.

Various measures have been undertaken by the Government to control such incidents are as under:

- (i) MeitY has communicated to all Banks and Payment Service Providers to undertake awareness campaigns for promotion of secure payment practices.
- (ii) Customer awareness campaigns are carried out by ecosystem players in order to ensure that customers do not fall victim to frauds using social engineering techniques.
- (iii) Reserve Bank of India (RBI) has issued instructions to banks (Scheduled Commercial Banks including RRBs, Small Finance Banks, Payments Banks, Primary (urban), State and District Central Co-operative Banks) regarding limiting the customer liabilities in unauthorised/ fraudulent electronic transactions.
- (iv) RBI has issued the “Master Direction on Digital Payment Security Controls” vide circular dated February 18, 2021 to all Scheduled Commercial Banks, Small Finance Banks, Payments Banks and NBFCs, for providing necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

(c): The RBI has mandated that all new cards issued by banks - debit and credit, domestic and international - be EMV chip and PIN based cards, to safeguard against cloning of ATM cards.

(d): The Department of Telecommunications has initiated steps for effective handling of Unsolicited Commercial Communication (UCC) and the financial frauds being done through misuse of telecom resources and development of redressal mechanism to enable telecom subscribers to lodge their complaints related to matters involving UCC.
