GOVERNMENT OF INDIA
MINISTRY OF FINANCE
LOK SABHA
UNSTARRED QUESTION NO-2241
ANSWERED ON- 02/08/2021

CASES OF FRAUD TRANSACTIONS

2241. SHRI P.C. MOHAN

Will the Minister of FINANCE be pleased to state:-

(a) whether it is true that with the increasing digitalisation in the country, there is steady increase in the cases of fraud in transactions;

(b) if so, the details of losses incurred due to increasing cyber fraud cases, State-wise; and

(c) the action taken by the Government to stop such actions and the results of such steps?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) and (b): As per Reserve Bank of India (RBI) data on frauds reported by Scheduled Commercial Banks 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 by 23.8% during the financial year 2020-21 from such amount for the preceding financial year.

(c): A number of measures have been taken to prevent cyber frauds, including, *inter alia*, the following:

(1) Indian Cyber Crime Coordination Centre has been established to provide a framework and ecosystem for law enforcement agencies (LEAs) for dealing with cybercrimes (including frauds related to credit cards, debit cards, online banking, etc.) in a comprehensive and coordinated manner.
(2) A National Cyber Crime Reporting Portal has been launched 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.
(3) Financial Cyber Fraud Reporting and Management System module has been launched for immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters.

(4) The Indian Computer Emergency Response Team (CERT-IN) 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.

(5) CERT-In is providing the requisite leadership for the CSIRT-Fin (Computer Security Incident Response Team-Finance Sector) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

(6) RBI has advised banks to have in place a Board-approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats.

In addition, RBI, to protect customers from fraud in digital transaction, has advised banks to take, *inter alia*, the following security and risk mitigation measures:

(1) For securing card transactions, inclusive of online alerts for all transactions, certification of merchant terminals, and conversion of magnetic strip cards to EMV chip and PIN cards;

(2) Capping the value/mode of transactions/beneficiaries, setting daily limits and issuing alerts upon addition of beneficiaries;

(3) Requiring PIN entry for all ATM transactions, and enabling all ATMs for processing EMV chip and PIN cards;

(4) For securing Prepaid Payment Instruments (PPIs) also referred to as 'wallets', informing customers in case the same login is provided for PPI and other services offered by PPI issuers, having restrictions on multiple invalid attempts to log into PPI and introducing time-out features, authenticating every wallet payment transaction by customer consent, in additional factor of authentication for debit cards, provision of customer-induced options for capping the number and value of transactions, provision of suitable cooling period for funds transfer on opening of PPI, and issue of alerts for PPI transactions; and

(5) To ensure that all new debit and credit cards are issued only for domestic usage unless international use is specifically sought by the customer.

*****