

GOVERNMENT OF INDIA  
MINISTRY OF FINANCE  
**RAJYA SABHA**  
**UNSTARRED QUESTION NO-535**  
ANSWERED ON- 07/02/2023

**FORENSIC ACCOUNTING IN DIGITAL ERA**

535. SHRI ANIL DESAI

Will the Minister of FINANCE be pleased to state:-

- (a) whether it is a fact that, due to the increase in multiple fraud techniques in the banking sector, newer methods have been adopted to cheat the common banking customers;
- (b) if so, the details of the crime data of the same for the last three years;
- (c) the remedial measures taken by banking authorities to train its employees to understand the seriousness of the crime and to prevent it; and
- (d) whether qualified experts in this new field are available, if so, the details thereof?

**ANSWER**

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) to (d): Digitalisation of banking services has helped banks in increasing efficiency, reach and competitiveness, and has also facilitated financial inclusion of unbanked. It has also helped in delivery of prompt and better customer services. At the same time, nature of risks associated has also changed and with the constant advancement in technology, new fraud techniques are being adopted by fraudsters. As per inputs received from the Reserve Bank of India (RBI), the recent methods of cyber frauds impacting the customers of banking sector majorly include, *inter alia*, Social Engineering attack, Phishing, Vishing, Distributed Denial of Service (DDoS) attack, Credential Compromise, Ransomware attack.

The National Crime Records Bureau (NCRB) collects data for crime in India from States and Union Territories, and publishes the same periodically. As per NCRB, the latest published data pertains to the year 2021, and 6229, 10,395 and 14,007 cases under frauds for cybercrime were registered during the years 2019, 2020 and 2021 respectively. These include frauds related to Credit/Debit/ATM cards, online banking, OTP, *etc.*

With regard to training of employees, a number of measures have been taken which include, *inter alia*, the following:

- (i) The Master Direction on Digital Payment Security Controls, issued by RBI in 2021, mandates that the staff, especially in the fraud control function, shall be trained in the specified skills and areas of expertise.
- (ii) A comprehensive circular on Cyber Security Framework in Banks issued by RBI in 2016 require banks, *inter alia*, to create awareness and take suitable steps in building the awareness among staff at all levels.
- (iii) With a view to enhance the management's awareness in banks with regard to IT and cyber security issues, officials of the banks (including Board Members, Senior Management team, Officers handling IT/IS assets) have been mandated to undergo training and certification programs conducted by Institute for Development and Research in Banking Technology in the concerned area.
- (iv) RBI also conducts workshops on "Fraud Risk management and Reporting in Banks" for officials of commercial banks and small financial banks with special emphasis on the vital area of focus for officials involved in credit monitoring and fraud prevention in the banks.
- (v) RBI has published on its website, BE(A)WARE – a booklet on the common *modus operandi* used by fraudsters and precautions to be taken while carrying out various financial transactions.
- (vi) Banks also circulate *modus operandi* of fraud cases, as received through Indian Banks Association, to the field to sensitise its officers/staff and create alertness against similar attempts.

RBI has apprised that qualified experts are available and are engaged by the supervised entities to oversee related functions. Further, as per inputs received from public sector banks, support of law enforcement agencies and experienced professionals are taken for conducting the training programs for their officials, and bank's faculty members are also provided training at reputed institution.

\*\*\*\*\*