GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO: 1357

ANSWERED ON TUESDAY, 11 MARCH, 2025/ 20 PHALGUNA, 1946 (SAKA)

INCREASE IN INCIDENCE OF CYBER FRAUDS

1357 SHRI C. Ve. SHANMUGAM:

Will the Minister of Finance be pleased to state:

(a) whether it is a fact that cyber security had been compromised and frauds had been increased, due to large number of banking transactions;
(b) if so, the details thereof;
(c) the steps taken by Government to ensure safe transactions without compromising on cyber security; and
(d) further measures taken by Government to instill confidence in the public about online transactions?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a) to (d): With increasing digital payment transactions in the country, incidences of fraudulent practices including digital financial frauds have also gone up in the last few years. As informed by the Reserve Bank of India (RBI), the details of frauds including amount involved as reported by the banks under the category 'Card / Internet and Digital Payments' during the FY 2020-21 to FY 2024-25 (till Dec'24) are as below:

FY	Number of Frauds(amount involved ₹1 Lakh and above)	Total Amount Involved in ₹ Crore
2020-21	2545	119
2021-22	3596	155
2022-23	6699	277
2023-24	29082	1457
2024-25 (till Dec'24)	13384	534

Source: RBI

RBI has issued Master Directions on Digital Payment Security Controls in February, 2021 to combat web and mobile app threats. These guidelines mandate the banks to implement a common minimum standards of security controls for various payment channels like internet, mobile banking, card payment etc. RBI has also launched an Artificial Intelligence (AI) based tool 'MuleHunter' for identification of money mule and advised the banks and financial institutions for its uses.

Further, in order to prevent frauds related to UPI transaction, National Payments Corporation of India(NPCI) has implemented device binding between mobile number and the device, two-factor authentications through PIN, daily transaction limit, limits and curbs on use cases etc. NPCI also provides a AI / Machine Learning (ML) based fraud monitoring solution to all the banks to generate alerts and decline transactions.

RBI and Banks have been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of 'cyber-crime'. Further, RBI has been conducting electronic-banking awareness and training (e-BAAT) programmes which focuses on awareness about frauds and risk mitigation.

In order to facilitate the citizens to report cyber incidents including illegal loan apps, MHA has launched a National Cybercrime Reporting Portal (www.cybercrime.gov.in) as well as a National Cybercrime Helpline number "1930"." Similarly, Department of Telecommunications has launched 'Chakshu' facility which facilitates citizens to report suspected fraud communication received over call, SMS or WhatsApp with the intention of defrauding like KYC expiry or update of bank account, etc.

To help customers recover the loss on account of fraudulent transactions, RBI vide circular dated 6th July, 2017 issued instructions to the banks on limiting the liability of customers (viz. Zero liability, Limited liability and Liability as per Board approved policy) in cases of unauthorised electronic banking transactions.

******