

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO: 1991
ANSWERED ON THE TUESDAY, 18 MARCH, 2025/ 27 PHALGUNA, 1946 (SAKA)

DIGITAL FINANCIAL FRAUD

1991 SHRI SANT BALBIR SINGH

Will the Minister of FINANCE be pleased to state:

- (a) the total number of reported cases of digital financial fraud, including incidents related to online banking, Unified Payments Interface (UPI), and financial application frauds, during the financial years 2022-25;
- (b) the proactive measures undertaken by financial regulatory bodies, such as the Reserve Bank of India (RBI) and other relevant agencies, to detect, prevent, and mitigate emerging digital financial fraud techniques; and
- (c) the effectiveness of existing cybercrime reporting platforms, including the National Cyber Crime Reporting Portal and dedicated financial fraud helplines, in resolving complaints and assisting victims in recovering lost funds?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a): 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. Reserve Bank of India (RBI) has implemented a Central Payments Fraud Information Registry (CPFIR), a web-based payment related fraud reporting solution, wherein all payment-related frauds are reported by banks, non-bank PPI issuers and non-bank credit card issuers. The details of frauds as reported on CPFIR during the FY 2022-23 to FY 2024-25 (till Jan, 25) are as below:

FY	Number of Incidents (in lakhs)	Total Amount Involved in ₹ Crore
2022-23	19.94	2537
2023-24	28.22	4403
2024-25 (till Jan, 25)	23.89	4245

Source: RBI

(b): In order to prevent digital financial frauds, various initiatives have been taken up by the Government, Reserve Bank of India (RBI) and National Payments Corporation of India (NPCI) from time to time. 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.

Similarly, NPCI has also implemented device binding between customer mobile number and the device, two factor authentications through PIN, daily transaction limit, limits and curbs on use cases etc to secure UPI transactions. NPCI also provides a fraud monitoring solution to all the banks to generate alerts and decline transactions by using AI/ML based models. RBI and Banks have also been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of 'cyber-crime' etc.

(c): The MHA has launched the National Cyber Crime Reporting portal (<https://cybercrime.gov.in>) to enable the public to report all types of cyber crimes. Cyber crime incidents reported on this portal are routed automatically to the respective State/UT law enforcement agency for further handling as per the provisions of law. The 'Citizen Financial Cyber Fraud Reporting and Management System' has been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters and so far, an amount of Rs. 4386 Crore (approx..) has been saved involving 13.36 lakh complaints.
