

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO 3596
ANSWERED ON TUESDAY, MARCH 24, 2026/ 3 CHAITRA, 1948 (SAKA)

FINANCIAL CYBER CRIME

3596 # SHRI MADAN RATHORE:

Will the Minister of Finance be pleased to state:

- (a) whether it is in the cognisance of Government that with the increasing use of digital payments in the country, incidents of cyber financial crimes are also rising;
- (b) the total amount lost in banking fraud cases during the last three years;
- (c) whether Government is going to introduce new technological arrangements in order to protect digital transactions; and
- (d) the steps being taken to strengthen coordination with States for prevention of cyber financial crimes?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a) & (b): With increasing digital payment transactions in the country, incidence of cyber frauds including digital payment frauds have also gone up in the last few years. As informed by the Reserve Bank of India(RBI), the number of digital payment frauds and amount involved during the last 3 years are as under:

FY	Volume (Lakh)	Value (in ₹ Crore)
2023-24	28.22	4403
2024-25	27.56	4824
2025-26(till January 2026)	24.17	3775
Grand Total	79.95	13002

(c): The Government in consultation with regulators and other stakeholders have been taking various initiatives from time to time to protect digital transactions, which inter alia include:

- (i) RBI has launched an Artificial Intelligence (AI) based tool 'MuleHunter' for identification of money mule and advised the banks and financial institutions for its uses.
- (ii) Banks have been advised to ensure deployment and adoption of robust software for real-time transaction monitoring and use of AI / ML tools in detecting suspicious and fraudulent transaction patterns as well as use of network analytics in identifying mule networks.

(iii) REs have also been advised to have a dedicated analytics set up that shall extensively monitor and analyse transactions, more specifically the transactions carried out through digital platforms and applications, in order to identify unusual patterns and activities which could alert them timely in initiating appropriate measures towards prevention of fraudulent activities.

(iv) Indian Digital Payment Intelligence Corporation (IDPIC) has been incorporated as section 8 company, under the Companies Act, 2013 on 16/10/2025. Its primary mandate is to detect, prevent, and analyse fraud in India's rapidly expanding digital payments ecosystem in real time by leveraging cutting-edge technologies, including Artificial Intelligence (AI), Machine Learning (ML), and Big Data Analytics.

(v) RBI and banks have also been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of 'cyber-crime' etc.

(vi) In order to prevent frauds related to Unified Payments Interface(UPI) transaction, measures such as device binding , two-factor authentications, daily transaction limit, limits and curbs on use cases etc. have been implemented. National Payments Corporation of India (NPCI) also provides a Artificial Intelligence(AI) / Machine Learning (ML) based fraud monitoring solution to all the banks to generate alerts and decline transactions.

(vii) 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.

(d): Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber-crime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of LEAs.

A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at Indian Cyber Crime Coordination Centre, Ministry of Home Affairs (MHA) where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.
