

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA
UNSTARRED QUESTION NO:1647
ANSWERED ON THE MONDAY, 10 MARCH, 2025/PHALGUNA 19, 1946 (SAKA)

QUANTUM OF LOSS TO PUBLIC DUE TO CYBER FRAUDS

1647. SHRI S VENKATESAN:

Will the Minister of FINANCE be pleased to state:

- (a) the quantum of loss to the public due to Cyber frauds during the last ten years;
- (b) the number of cases which have been reported during the last five years;
- (c) the number of culprits which have been arrested along with the number of FIRs filed during the last five years;
- (d) whether all the complainants have been attended and the victims have been penalised; and
- (e) if so, the details thereof along with the steps taken by the Government to prevent such frauds?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a) to (e): With increasing digital payment transactions in the country, incidences of fraudulent practices including digital payment frauds have also gone up in the last few years.

The Reserve Bank of India (RBI) has informed that they do not maintain such information, however, the year-wise number of frauds, and extent of loss as reported by the Commercial Banks and all India Financial Institutions under the category 'Card / Internet and Digital Payments' during the period FY 2014-15 to FY 2024-25 (till Dec'24) are as below:

FY	Number of Frauds (amount involved ₹1 Lakh and above)	Extent of Loss (in ₹ Crore)
2014-15	845	18.46
2015-16	1191	26.90
2016-17	1372	27.78
2017-18	2058	79.79
2018-19	1866	51.74
2019-20	2677	44.22
2020-21	2545	50.10
2021-22	3596	80.33
2022-23	6699	69.68
2023-24	29082	177.05
2024-25 (till Dec'24)	13384	107.21

Source: RBI

‘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 their LEAs.

RBI has issued Master Directions dated July 15, 2024, on Fraud Risk Management for the Regulated Entities which provides for framework on Early Warning Signals (EWS) to monitor transactions / unusual activities in the non-KYC compliant and money mule accounts etc. Further, the requirement for data analytics and Market Intelligence Unit have been mandated for the supervised entities for monitoring transactions, specifically the transactions through digital platforms and applications.

To spread awareness against cyber-crimes, the Government has been taking various initiatives from time to time. These, inter alia, includes cyber safety tips through social media accounts, publishing of handbook for adolescents/students, publishing of ‘Information Security Best Practices’ for the benefit of government officials, organizing cyber safety and security awareness weeks in association with States/Union Territories etc. RBI and banks have also been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of ‘cyber-crime’ etc.

The Indian Computer Emergency Response Team (CERT-In) takes various measures for safe usage of digital technologies and prevent cyber frauds through issuance of alerts and advisories, Cybersecurity mock drills to enable assessment of cyber security posture and preparedness of organisations.

In order to facilitate the citizens to report any cyber incidents including financial frauds, Ministry of Home Affairs (MHA) has also 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 Digital Intelligence Platform (DIP) and ‘Chakshu’ facility on Sanchar Saathi portal (<https://sancharsaathi.gov.in>). ‘Chakshu’ 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.
