GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES
RAJYA SABHA
UNSTARRED QUESTION NO-1185

ANSWERED ON TUESDAY, FEBRUARY 10, 2026/ 21 MAGHA, 1947 (SAKA)

BANK FRAUD CASES AND CYBER FINANCIAL CRIMES IN ODISHA

1185. SHRI MANAS RANJAN MANGARAJ:

Will the Minister of FINANCE be pleased to state:-

(a) the number of bank fraud cases and cyber financial frauds reported in Odisha during the last three years, year-wise;

(b) the total amount involved and amount recovered in such cases; and

(c) the steps taken to strengthen banking security, customer awareness and fraud prevention in Odisha?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE
(SHRI PANKAJ CHAUDHARY)

(a) to (c): As per the Reserve Bank of India (RBI) data, the details of bank frauds as reported by Scheduled Commercial Banks (SCBs) and All India Financial Institutions (AIFIs), including cyber financial frauds, based on the date of occurrence in the state of Odisha, during the last three financial years (FY), are as under:

(Amounts in crore Rs.)

FY 2022-23			**FY 2023-24**			**FY 2024-25**		
Number	Amount Involved	Amount Recovered	Number	Amount Involved	Amount Recovered	Number	Amount Involved	Amount Recovered
1,594	255.35	10.16	2,363	1,155.68	4.57	919	31.47	8.86

Further, RBI has apprised that state-wise data for cyber fraud category is not maintained by it.

Steps taken by the Government and the Reserve Bank of India (RBI) over the last few years to prevent and to deter instances of bank frauds, strengthen banking security and customer awareness include, *inter alia*, the following:

(i) An online searchable database of frauds reported by banks, in the form of Central Fraud Registry, has been set up by the RBI to enable timely identification, control and mitigation of fraud risk.

(ii) Under the PSB Reforms Agenda, comprehensive and automated Early Warning Systems (EWS) were instituted in PSBs, with approximately 80 EWS triggers and use of third-party data for time-bound remedial actions in the borrowing accounts to proactively detect stress and in turn reducing slippage into NPAs.

(iii) The Fugitive Economic Offenders Act has been enacted to provide for measures to deter fugitive economic offenders from evading the process of law in India by staying outside the jurisdiction of Indian courts.

(iv) RBI has issued revised instructions to banks *vide* its Commercial Banks - Responsible Business Conduct, Directions, 2025 regarding limiting the customer liability in unauthorized electronic banking transaction from a customer protection perspective.

(v) Several initiatives have been taken to spread awareness amongst customers, which *inter alia* include, dissemination of messages on cyber-crime through short message service (SMS), radio campaigns, publicity on prevention of cyber-crime and cyber safety tips through social media accounts of the Indian Cybercrime Coordination Centre (I4C), conducting of electronic-banking awareness and training (e-BAAT) programmes by RBI.

(vi) PSBs have been advised to obtain certified copy of the passport of the promoters/directors and other authorised signatories of companies availing loan facilities of more than Rs. 50 crore.

(vii) Banks have been advised by RBI to report deficient third-party services (such as legal search reports, property valuers' reports, *etc.*) and collusion of these service providers with fraudsters to the Indian Banks' Association, which maintains a caution list of such service providers.

(viii) The I4C has operationalised Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) portal for immediate reporting of financial frauds and to stop siphoning-off of funds by the fraudsters.

(ix) Cyber Fraud Mitigation Centre (CFMC) has been established at I4C with representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and States/UTs Law Enforcement Agencies (LEAs) to work together for immediate action and seamless cooperation to tackle online financial crimes.

(x) Seven Joint Cyber Coordination Teams (JCCTs) have been formed to foster a close cooperation among LEAs during interstate cybercrime investigations. It focuses on operational cooperation in parallel investigations in various States/UTs.

(xi) National Cyber Forensic Laboratory has been setup as a facility for forensic analysis and investigation of cybercrime by use of the latest digital technology to support investigations undertaken by LEAs.

*****