

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION No. 6122**  
TO BE ANSWERED ON 01.04.2026

**RISE IN FRAUD AND FINANCIAL SCAMS LINKED TO UPI**

**6122. SHRI ADHIKARI SOUMENDU:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government has noted a rise in fraud and financial scams linked to the Unified Payments Interface (UPI) where the transaction touched a record value of Rs. 230 lakh crores in Financial Year 2025-26;
- (b) if so, the total number of such incidents reported annually and the estimated financial losses incurred by users during the last three fiscal years, therefor;
- (c) the measures undertaken by the Government and the action taken by the National Payments Corporation of India (NPCI) to strengthen the security architecture of UPI transactions and prevent fraudulent activities thereof; and
- (d) total defrauded funds from such incidents have been successfully safeguarded or returned to cyber complaints victims since 2023-24 Financial Year to till date therein?

**ANSWER**

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY  
(SHRI JITIN PRASADA)

(a) to (d): The Government is working in line with the Hon'ble Prime Minister's vision of democratising technology and enabling its use at population scale. It has expanded access to the internet and made it more affordable.

The Digital Public Infrastructure (DPI) approach is a key pillar of this approach. It has enabled service delivery at scale through open, interoperable and secure platforms such as Aadhaar, UPI and DigiLocker.

**Rising UPI transactions**

Unified Payments Interface (UPI) is India's real-time digital payment system. It handled 20.394 billion transactions worth 26.842 lakh crore in February 2026.

With the increasing digital payment transactions in the country, incidences of frauds and financial scams have also been reported. To strengthen the security of UPI transactions and prevent fraud, Government has taken several measures such as:

- Device binding between user's mobile number and device

- Two-factor authentication (UPI PIN) for all transactions
- Transaction limits and use-case restrictions
- AI/ML-based fraud detection systems deployed by NPCI and banks
- Real-time monitoring and alert systems to detect suspicious transactions

NPCI has also enabled fraud monitoring solutions for banks and facilitates real-time data sharing with the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs. This has enabled timely identification of fraudulent accounts and preventive action.

Further, awareness campaigns are regularly conducted by RBI, banks and Government agencies through SMS alerts, media outreach and public advisories to educate users on safe digital practices.

In addition, the National Cyber Crime Reporting Portal ([cybercrime.gov.in](http://cybercrime.gov.in)) and helpline 1930 have been operationalised to enable immediate reporting of financial frauds. This has helped in ensuring timely action for blocking and recovery of defrauded funds, in coordination with banks and law enforcement agencies.

These measures collectively aim to strengthen the security architecture of UPI, minimise fraud risks and enhance user protection in digital payments.

\*\*\*\*\*

