

**GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS**

**LOK SABHA
UNSTARRED QUESTION NO. 915
TO BE ANSWERED ON 4TH FEBRUARY, 2026**

FINANCIAL FRAUD RISK INDICATOR (FRI)

**†915. SHRI TEJASVI SURYA:
DR. RAJESH MISHRA:
SHRI NEERAJ MAURYA:
SMT. SHOBHANABEN MAHENDRASINH BARAIYA:
SHRI DEVESH SHAKYA:
SHRI BALABHADRA MAJHI:
SHRI YADUVEER WADIYAR:
SHRI DAMODAR AGRAWAL:
SMT. APARAJITA SARANGI:
SHRI CHANDRA PRAKASH JOSHI:
SHRI SHANKAR LALWANI:**

Will the Minister of COMMUNICATIONS be pleased to state:

- (a) the measures taken by the Government to prevent the misuse of telecommunications resources and to protect against cyber fraud;
- (b) the outcomes achieved by the Government through initiatives such as Sanchar Saathi, the financial Fraud Risk Indicator (FRI) and the Digital Intelligence Platform in preventing the misuse of telecommunications resources and safeguarding against cyber fraud including the number of cases detected, blocked and resolved in the State of Odisha;
- (c) the extent and the manner in which coordination is being undertaken by the Government with banks and law enforcement agencies for real-time detection of fraud and prompt action with specific details of such coordination mechanisms joint action undertaken in Odisha;
- (d) the steps taken by the Government to strengthen the resilience of telecommunications systems using indigenous technologies such as Broadcasting Cell during disasters and to strengthen public warning systems; and whether those systems have been implemented, listed or operationalised in disaster-prone areas of Odisha; and
- (e) the future roadmap proposed by the Government to further strengthen digital trust, cyber security and citizen awareness in the rapidly expanding telecommunications ecosystem?

ANSWER

**MINISTER OF STATE FOR COMMUNICATIONS AND RURAL DEVELOPMENT
(DR. PEMMASANI CHANDRA SEKHAR)**

(a) to (c) Department of Telecommunications (DoT) has undertaken the following measures to prevent the misuse of telecommunications resources and to protect citizens against cyber fraud on pan India basis including Odisha:

- i. DoT has developed Sanchar Saathi, a citizen centric initiative, available as web portal (www.sancharsaathi.gov.in) and mobile App, which facilitates citizens to report suspected fraud communications, to know mobile connections in their name, to report lost/ stolen mobile handsets, to check genuineness of mobile handset etc. Through Sanchar Saathi, 8.33 lakh lost/ stolen mobile handsets have been recovered, 2.24 crore mobile connections, reported by the citizens as 'Not My Number' or 'Not Required', have been disconnected and 39.44 lakh mobile connections have been disconnected based on 7.7 lakh inputs provided by the citizens related to suspected fraud communications.
 - ii. DoT and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers. The system has resulted in almost 99% reduction in such call attempts.
 - iii. DoT has developed an indigenous Artificial Intelligence (AI) and Big data Analytics tool ASTR to identify SIMs taken by same person in different names. Based on ASTR, more than 88 lakh mobile connections have been disconnected failing reverification.
 - iv. DoT has established Digital Intelligence Platform (DIP), a secure online platform, for bi-directional information sharing with stakeholders for prevention of misuse of telecom resources in cyber-crimes and financial frauds. More than 1200 organizations have been on-boarded on DIP including central security agencies, 36 State/UT Police, Indian Cyber Crime Coordination Centre (I4C), 1100 Banks, Unified Payments Interface (UPI) service providers, Payment System Operators (PSOs), Telecom Service Providers (TSPs), WhatsApp etc.
 - v. DoT has developed Financial Fraud Risk Indicator (FRI) which is a risk-based metric that classifies a mobile number to have been associated with medium, high, or very high risk of financial fraud. Based on FRI, the stakeholders like Banks and UPI service providers initiate necessary action as per their analysis on the associated accounts /profiles in their respective domain. As reported by stakeholders, total fraud amount prevented based on transaction decline and alert/notifications given to the citizens is more than ₹1000 crores.
- (d) Public warning systems for disaster management have been strengthened through the nationwide implementation of Common Alerting Protocol (CAP)-based integrated alert system, using indigenous solutions, enabling timely, geo-targeted, and multilingual dissemination of emergency alerts in close coordination with disaster management authorities, alert generating agencies and alert disseminating agencies including TSPs.
- (e) DoT has made a T-CSIRT framework which is sectoral incident response and cyber security coordination function for telecommunication ecosystem. Its core purpose is to enable timely detection, analyze, coordinate and mitigate cyber incidents and vulnerabilities impacting telecom networks of TSPs, also comprising of Critical Telecom Infrastructure.

DoT is actively promoting digital safety and preventing telecom-related frauds through widespread multilingual awareness campaigns including social media platforms, news articles, digital screens, hoardings in public spaces, TV & radio messages, SMS campaigns, student volunteers through *Sanchar Mitra* scheme etc.
