GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

LOK SABHA
UNSTARRED QUESTION NO. 1978
TO BE ANSWERED ON 11TH FEBRUARY, 2026

PROTECTION OF CRITICAL TELECOM INFRASTRUCTURE AND REDUCTION OF TELECOM FRAUD

1978. SHRI P V MIDHUN REDDY:

Will the Minister of COMMUNICATIONS be pleased to state:

(a) the details of the strategy of the Government to protect critical telecom infrastructure and address fraud vectors such as SIM misuse, illegal gateways, call spoofing and related cyber-enabled offences;

(b) whether any targeted or enhanced measures have been deployed in Andhra Pradesh following recent large-scale telecom and financial fraud cases and if so, the details thereof;

(c) the details of the key performance indicators or metrics used by the Government to assess effectiveness in fraud reduction and user protection; and

(d) the steps taken to strengthen coordination with law enforcement agencies, telecom service providers and financial institutions to prevent recurrence of such frauds and protect citizens from financial losses?

ANSWER

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

(a) To protect critical telecom infrastructure and address fraud vectors such as SIM misuse, illegal gateways, call spoofing and related cyber-enabled offences, Government has taken several measures, inter-alia, including the following –

I. Section 42 of the Telecommunications Act, 2023 prescribes following as an offence:

   i. providing telecommunication services or establishing telecommunication network without authorisation or causing damage to critical telecommunication infrastructure.
   ii. obtaining Subscriber Identity Modules (SIMs) or other telecommunication identifiers through fraud, cheating or personation.
   iii. possessing radio equipment without an authorisation or an exemption that can accommodate more than specified number of SIMs.
   iv. tampering with telecommunication identifiers or willfully possessing radio equipment knowing that it uses unauthorised or tampered telecommunication identifiers.

II. The Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 have been notified on 22.11.2024 prescribing standards, security practices, upgradation requirements and procedures for Critical Telecommunication Infrastructure (CTI).

(b) & (c) The measures undertaken by Department of Telecommunications (DoT) to prevent the misuse of telecommunications resources and to protect citizens against cyber fraud on pan India basis, including Andhra Pradesh (AP) and their effectiveness is as follows:

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. The key performance indicators of actions initiated based on Sanchar Saathi are provided in table below:

Parameter	**All India figures**	**AP Licensed Service Area (includes the states of AP and Telangana)**
Recovery of lost/ stolen mobile handsets	8.46 lakhs	1.63 lakhs
Mobile connections disconnected based on reporting by the citizens as 'Not My Number' or 'Not Required'	2.28 crores	21.5 lakhs
Mobile connections disconnected based on inputs provided by the citizens related to suspected fraud communications	39.53 lakhs	3.46 lakhs

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 developed Financial Fraud Risk Indicator (FRI) which is a risk-based metric that categorizes a suspicious mobile number according to its probability of being associated with medium, high, or very high risk of financial fraud. FRI empowers stakeholders – especially banks, Non-Banking Financial Companies (NBFCs), and UPI service providers – to prioritize enforcement and take additional customer protection measures like enhanced due diligence and adoption of necessary real-time response protocols (alerts, transaction delays, warnings, transaction decline etc.) for flagged mobile numbers. Since its launch in May 2025, financial institutions have reported that based on transaction decline and alert/notifications given to the citizens, potential frauds amounting to more than ₹1400 crores have been prevented utilizing FRI.

(d) 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), Banks, Unified Payments Interface (UPI) service providers, Payment System Operators (PSOs), and Telecom Service Providers (TSPs).

*****