GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

RAJYA SABHA
STARRED QUESTION NO. 141
TO BE ANSWERED ON 12TH FEBRUARY, 2026

REDUCTION IN CYBER/TELECOM FRAUDS

141 # SHRI NEERAJ DANGI:

Will the Minister of Communications be pleased to state:

(a) the number of fake/suspected connections or accounts identified and acted upon so far through the Digital Intelligence Platform;

(b) whether there is reduction in cyber/telecom frauds attributable to this Platform and if so, the details thereof;

(c) the Ministries/Departments and agencies that have been integrated with the Platform; and

(d) the nature of data being collected through the said Platform and the safeguards put in place to ensure data security and privacy?

ANSWER

MINISTER OF COMMUNICATIONS AND DEVELOPMENT OF NORTH EASTERN REGION
(SHRI JYOTIRADITYA M. SCINDIA)

(a) to (d) A statement is laid on the Table of the House.

STATEMENT TO BE LAID ON THE TABLE OF RAJYA SABHA IN RESPECT OF PARTS (a) TO (d) OF THE RAJYA SABHA STARRED QUESTION NO. 141 FOR 12TH FEBRUARY, 2026 REGARDING "REDUCTION IN CYBER/TELECOM FRAUDS."

(a) to (c) The Department of Telecommunications (DoT) has developed 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 1,200 organisations have been on-boarded on DIP, including central security agencies, Police departments of 36 States and Union territories, Indian Cyber Crime Coordination Centre (I4C), banks, Unified Payments Interface (UPI) service providers, payment system operators and Telecom Service Providers (TSPs).

DIP enables on-boarded stakeholders to share mobile numbers suspected to be misused in cybercrime and financial frauds with DoT. Data shared by stakeholders is analysed by DoT. Major outcomes are as follows:

(i) *ASTR:* This is an artificial intelligence and big data analytics tool that identifies suspicious mobile connections. Such numbers are shared with TSPs through DIP. More than 88 lakh such mobile connections have been disconnected after failing reverification.

(ii) *International Incoming Spoofed Calls Prevention System (CIOR):* This is a system to identify and block incoming international spoofed calls displaying Indian mobile numbers that appear to be originating within India. Since its commissioning on 17.10.2024, CIOR has shown significant results, blocking 1.35 crore calls in 24 hours and has resulted in nearly 99% reduction in spoofed calls with Indian calling line identification. Calls that still land on international gateways are blocked there itself.

(iii) *Financial Fraud Risk Indicator (FRI):* This is a risk-based metric that categorises 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 prioritise 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 or notifications given to citizens, potential frauds amounting to over ₹1,400 crore have been prevented utilising FRI.

(iv) Based on 7.93 lakh reports of suspected fraud communication shared by citizens on Sanchar Saathi, 39.53 lakh mobile connections have been disconnected.

(d) The analysis based on the data is shared by DoT with stakeholders on DIP in the form of a mobile number revocation list, which is a list of disconnected mobile numbers along with the reasons and date of disconnection, and FRI. Stakeholders, in return, share action taken reports and also mobile numbers suspected to be misused in cybercrime and financial frauds. DIP is an online secure platform that ensures data security and privacy where access is granted based on strict, real-time authentication and authorisation. Further, necessary security safeguards based on industry best practices have been implemented through firewalls, multi-factor authentication, identity and access management and regular security assessments and audits.

****