GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

LOK SABHA
UNSTARRED QUESTION NO. 5405
TO BE ANSWERED ON 25TH MARCH, 2026

SANCHAR SAATHI 2.0 PORTAL/PLATFORM

†5405. SMT. ANITA NAGARSINGH CHOUHAN:

Will the Minister of COMMUNICATIONS be pleased to state:

(a) whether the Government has launched the 'Sanchar Saathi 2.0' portal/platform with the objective of providing protection to citizens against problems such as cyber fraud, mobile theft and fake SIM cards and if so, the key objectives and features thereof;

(b) whether the facilities for blocking/tracing mobile phones, identifying suspicious SIM cards and filing complaints by consumers are being provided through this platform;

(c) whether the Government has established coordination with Telecom Service Providers (TSPs), State Governments and Law Enforcement Agencies (LEAs) for the effective utilisation of the said portal; and

(d) if so, the details of the major steps taken and the future action plan of the Government to further strengthen citizen security and ensure effective control over digital fraud?

ANSWER

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

(a) & (b) Department of Telecommunications (DoT) has developed Sanchar Saathi, a citizen centric initiative, with the objective to prevent misuse of telecommunications resources in digital frauds. It is available as web portal (www.sancharsaathi.gov.in) and mobile App. Key features of Sanchar Saathi, inter-alia, includes facilitating citizens to report suspected fraud communications, to know mobile connections in their name & report connections which are not required or not taken by them, to report lost/ stolen mobile handsets, to check genuineness of mobile handset.

(c) DoT has developed Digital Intelligence Platform (DIP) which is 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 1,400 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).

(d) Along with Sanchar Saathi and DIP, some of the other prominent measures undertaken to strengthen citizen security & ensure effective control over digital fraud are as follows:

i. *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 from within India. Such calls are, inter-alia, being misused to impersonate government officials in cyber-frauds like digital-arrests.

ii. *ASTR:* This is an artificial intelligence and big data analytics tool that identifies suspicious mobile connections. Such numbers are shared with TSPs through DIP.

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.

*****