GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

RAJYA SABHA
UNSTARRED QUESTION NO. 502
ANSWERED ON 24TH JULY, 2025

FAKE CALLS AND SMS SCAMS

502 SHRI C. VE. SHANMUGAM:

Will the Minister of Communications be pleased to state:

(a) whether Government is aware of the growing menace of fake calls and SMS scams in the country;

(b) if so, the details of such incidents reported during the last year, including the number of cases, regions most affected and the estimated financial loss caused by these scams;

(c) the measures being taken to stop the issue of fake calls and SMS scams particularly using advanced technology to deceive the public;

(d) whether Government intends to create awareness and to educate the public about identifying and avoiding such fraudulent activities;

(e) if so, the details thereof; and

(f) further steps taken in this regard?

ANSWER

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

(a) to (c) Matters relating to Cyber Crime are under the Ministry of Home Affairs (MHA) as per allocation of the business rules. Department of Telecommunications (DoT) undertakes efforts to prevent misuse of telecom resources for cyber frauds. Further, 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. MHA has established the Indian Cyber Crime Coordination Centre (14C) as an attached office to provide a framework and eco-system for Law Enforcement Agencies (LEAs) to deal with cyber-crimes. MHA has also launched the National Cyber Crime Reporting Portal- NCRP (https://cybercrime.gov.in) to enable public to report all type of cybercrimes. As per I4C, total number of complaints on NCRP and amount lost were 19.18 lakh and 22811.95 crore respectively in 2024. Further, DoT and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers. These calls appear to be originating within India but were being made by the cyber-criminals from abroad by spoofing the Calling Line Identity (CLI). Further, for countering uptake of SIMs using fake documents, DoT has created an indigenous Artificial Intelligemce (AI) and Big data Analytic tool ASTR to identify SIMs taken by same person in different names.

(d) & (e) DoT actively engages with citizens to raise awareness about telecom-related frauds and for staying updated on the latest telecom safety measures. Efforts have also been made to encourage the use of the Sanchar Saathi App/portal, a citizen centric initiative of DoT for reporting suspected fraud communications. Engagement with citizens and awareness efforts have also been made through state-specific briefings & dissemination of content in local languages, social media campaigns, regular press releases, SMS campaigns and collaboration with multiple stakeholders like Law Enforcement Agencies (LEAs)/Banks/ Telecom Service Providers (TSPs) etc. Further, Through the Sanchar Mitra volunteer program of DoT, student volunteers from various universities are actively engaging with citizens to educate them about digital safety, fraud prevention, and Sanchar Saathi. They are conducting awareness drives, workshops, and on-ground interactions with public regarding securing their mobile connections and for reporting frauds.

(f) Further, steps taken by DoT, inter-alia, includes the following:

i. DoT has developed an online secure Digital Intelligence Platform (DIP) for sharing of information related to misuse of telecom resources among the stakeholders for prevention of cyber-crime and financial frauds. About 620 organizations have been onboarded on DIP including central security agencies, State/UT Police, I4C, Goods & Service Tax Network (GSTN), Banks, TSPs etc.
ii. 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. FRI empowers stakeholders-especially banks, NBFCs, and UPI service providers to prioritize enforcement and take additional customer protection measures in case a mobile number has high risk.

*****