GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

LOK SABHA
UNSTARRED QUESTION NO. 4139
ANSWERED ON 12TH AUGUST, 2026

AI/ML BASED UCC DETECT SYSTEM

4139. SHRI YADUVEER WADIYAR:

WILL the Minister of COMMUNICATIONS be pleased to state:

(a) the compliance status among all Access Service Providers (ASPs) regarding the mandatory deployment of AI/ML-based UCC Detect systems to proactively identify and flag Unsolicited Commercial Communications (UCC) without waiting for consumer complaints as per the recent TRAI directives;

(b) the technical evaluation metrics and auditing protocols established to ensure that operators successfully adhere to the strict 2-hour real-time window for sharing AI-flagged spam intelligence across the common Distributed Ledger Technology (DLT) blockchain platform; and

(c) the number of Unregistered Telemarketers (UTMs) and persistent corporate offenders whose telecom resources have been blocked, suspended or blacklisted under the new ‘four strikes in ten days" AI enforcement rule?

ANSWER

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

(a) to (c) Artificial Intelligence (AI) based systems for detecting Unsolicited Commercial Communications (UCC), through voice calls or SMS, or both, have been implemented by the four major Access Service Providers, namely M/s Bharti Airtel Limited, M/s Reliance Jio Infocomm Limited, M/s Vodafone Idea Limited, and M/s Bharat Sanchar Nigam Limited.

The Access Providers are presently sharing AI-flagged spam intelligence with one another through email. However, AI-based identification of suspected spam does not, by itself, constitute conclusive proof of UCC. Accordingly, the directions issued by the Telecom Regulatory Authority of India (TRAI) provide that such flagging shall be used to trigger further investigation by the concerned Access Providers against suspected senders.

Where five or more Calling Line Identities (CLIs) associated with a sender are flagged as suspected UCC CLIs within a period of ten days, the Access Provider is required to re-verify the sender’s Know Your Customer (KYC) details and take appropriate action in accordance with the extant KYC guidelines. In cases of repeated violations, the Access Provider is also required to undertake physical KYC verification of the suspected sender and examine whether telecom resources have been misused for sending UCC. If the sender is found to be misusing

telecom resources for UCC, the directions mandate outgoing barring or disconnection of the relevant telecom resources, along with blacklisting of the sender.

AI-based spam flagging systems deployed by Telecom Service Providers (TSPs) also enable consumers to exercise caution by either ignoring suspected spam communications or responding to them at their discretion. TSPs have commenced issuing warning notifications to entities suspected, with a high degree of probability, of sending spam. More than 2.43 lakh warning notifications were issued to suspected senders within one week of the commencement of this initiative on 23 June 2026.

*****