Dated: 27th February, 2026

DIRECTION

Subject: Direction under section 13, read with sub-clauses (i) and (v) of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997, regarding institutionalization of AI/ML-based UCC_Detect intelligence for inter-operator sharing and regulatory action against UCC senders.

File No. RG-25/(17)/2022-QoS (E-8557) — Whereas the Telecom Regulatory Authority of India (hereinafter referred to as "the Authority"), established under sub-section (1) of section 3 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) (hereinafter referred to as " TRAI Act"), has made the Telecom Commercial Communications Customer Preference Regulations, 2018 (6 of 2018), (hereinafter referred to as "regulations"), to regulate Commercial Communications (UCC);

2. And whereas sub regulation (9) of regulation 5 mandates access providers to detect, identify and take action against senders of commercial communications who are not registered with them;

3. And whereas regulation 8, read with Schedule IV to the regulations (hereinafter referred to as Schedule IV), mandates every Access Provider to establish, maintain and operate a UCC_Detect system for detection of bulk UCC senders;

4. And whereas sub-item (a) of item (1) of clause 1 of Schedule IV mandates identification of senders on the basis of signatures;

5. And whereas sub-item (d) of item (1) of clause 1 of Schedule IV mandates real-time sharing of UCC_Detect data and insights with other access providers over the Distributed Ledger Technology (DLT) platform;

6. And whereas sub-item (g) of item (1) of clause 1 of Schedule IV mandates identification of senders based on defined signals or trigger parameters and treatment of such senders as suspected Unregistered Telemarketers (UTMs);

वर्ल्ड ट्रेड सेंटर, टावर-एफ (चतुर्थ से सातवाँ तल), नौरोजी नगर, नई दिल्ली-110029
World Trade Center, Tower-F, (4th to 7th Floor), Nauroji Nagar, New Delhi-110029
Tel. : 011-26769600 / www.trai.gov.in

7. And whereas sub-item (i) of item (1) of clause 1 of Schedule IV mandates the use of advanced and reliable Artificial Intelligence (AI) and Machine Learning (ML) based technological solutions for proactive UCC detection, prevention and monitoring;

8. And whereas sub-item (f) of item (1) of clause 1 of schedule IV, inter alia, provides that UCC_Detect System shall have functionality of considering inputs available, if any, from any other network element(s) of the access provider system;

9. And whereas the Authority, in exercise of the powers conferred upon it under section 13, read with sub-clauses (i) and (v) of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), and the provisions of the regulations, vide its direction No RG-25/(6)/2022-QoS dated the 13th June, 2023, directed all the access providers, inter-alia, to deploy Artificial Intelligence and Machine Learning based UCC_Detect system which is capable of evolving constantly to deal with new signatures, new patterns and new techniques used by the Unregistered Telemarketers (UTMs);

10. And whereas several access providers have deployed AI/ML-based network-level UCC detection and alert systems and demonstrated their capability to analyze behavioral signatures including call and message volume, velocity, diversity, duration and temporal patterns, and to flag UCC in near real-time;

11. And whereas access providers have largely used the detection system, referred to in the preceding para, for subscriber-facing alertsbut are yet to institutionalize these outputs for investigation and enforcement against originating entities, considering the availability and demonstrated effectiveness of such AI/ML-based systems;

12. And whereas the Authority has observed that alerting of the subscriber without backend enforcement does not act as a deterrence and enforcement has, thus, remained predominantly complaint-driven;

13. And whereas from UCC complaint data, the Authority noted that approx. 85 percent UCC complaints are reported against Unregistered Telemarketers (UTMs);

14. And whereas effective containment of UTM-originated UCC requires a calibrated leveraging of AI/ML-based network intelligence deployed by access providers;

15. And whereas the Authority observes that Access Providers have deployed AI/ML-based UCC_Detect systems using a wide range of behavioral parameters;

16. Now, therefore, in exercise of powers conferred upon it under section 13, read with sub-clauses (i) and (v) of clause (b) of sub-section (1) of section 11, of TRAI Act, 1997, and the provisions of the Telecom Commercial Communications Customer Preference Regulations, 2018, the Authority hereby directs that-

(a) this Direction shall apply to all the Access Providers ;

(b) nothing in this Direction shall require disclosure of proprietary algorithms, source code, model architecture or internal risk-scoring methodologies of the AI-based UCC detection system deployed by any Access Provider;

(c) every Terminating Access Provider (TAP) shall, through its AI/ML-based UCC_Detect system, identify and flag the Calling Line Identification (CLI) of the sender as "Suspected UCC CLI" based upon the behavioural parameters as specified in the AI/ML-based UCC_Detect system. Immediately upon such flagging and in any case within two hours of such flagging, TAP shall share, through the Distributed Ledger Technology (DLT) platform, the flagged CLI with the concerned Originating Access Providers (OAPs);

(d) upon receipt of the flagged CLI from TAP, OAP shall immediately issue a notification, as per Annexure-I, through SMS or mail or both, to the sender associated with such CLI, informing that his CLI has been flagged as "Suspected UCC CLI";

(e) OAP shall, within one business day of the receipt of the flagged CLI from TAP, ascertain unique KYC identifiers of the sender associated with such CLI, using its subscriber records to enable all Access Providers to identify all the telecom resources allotted to such sender, and OAP shall, within the next one business day, share through DLT platform the unique KYC identifiers of such Sender with all other Access Providers who, within one business day of the receipt of such unique KYC identifiers from OPA, shall identify all the telecom resources allotted by them to such Sender;

(f) upon identification of all the telecom resources allotted to such Sender, as referred in the preceding para, all the Access Providers including OAP, shall examine, within next one business day, whether any other CLI allotted to the same Sender has been flagged as "Suspected UCC CLI" by their respective AI/ML-based spam alert systems during the preceding ten days, and all such flagged CLIs mapped to the same sender shall be recorded and shared on DLT platform by all the Access Providers on the same day;

(g) upon receipt of the data of all CLIs associated with such sender across the network, which have been flagged as "Suspected UCC CLI", all the concerned OAPs shall check, within one business day of the receipt of such data, whether five or more CLIs of the sender have been flagged as "Suspected UCC CLI" within a period of last ten days, and if it is found that five or more CLIs of the sender have been flagged as "Suspected UCC CLI" within the last ten days, all the concerned OAPs shall take action against the sender as follows:

(A) for the first such instance, OAP shall, within the next three business days, carry out the re-verification of KYC of the sender as per the licence conditions and take necessary action in accordance with the extant KYC guidelines;

(B) for the second such instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the provisions of the regulations, OAP shall take action against the sender as provided under clause (a) of sub-regulation 6 of regulation 25 of the regulations;

(C) for any such subsequent instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the

provisions of the regulations, OAP shall take action against the sender as provided under clause(b) of sub-regulation (6) of regulation 25 of the regulations.

17. All the Access Providers are directed to comply with the above directions within thirty days from the date of issue of this Direction.

27/2/26.

(Deepak Sharma)
Advisor (QoS-II)

To

All Access Providers

Annexure-I

The format of notification shall be as under:

"Your <call/ SMS> from the <number > has been flagged as suspected unsolicited commercial communication on the basis of pattern analysis. You are advised that commercial communication can only be made by registered senders or telemarketers in accordance with the TRAI regulations. If you are found to be engaged in sending unsolicited commercial communication, all your telephone connection across all the telecom service providers are liable for action including barring outgoing calls OR disconnection and blacklisting for one year. For any clarification, please call <number> or mail to <mail-id>"