Information Note to the Press

For Immediate Release

(Press Release No. 119/2026)

Telecom Regulatory Authority of India (TRAI)

TRAI Strengthens Framework for Curbing Unsolicited Commercial Communications through Technology-Driven Enforcement and Enhanced Consumer Protection

New Delhi, 18th September, 2026 – The Telecom Regulatory Authority of India (TRAI) has amended the Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR, 2018) to further strengthen the regulatory framework for curbing Unsolicited Commercial Communications (UCC), protect consumers from spam and prevent misuse of telecom resources for sending UCC.

2. TRAI issued "Draft Telecom Commercial Communication Customer Preference (Third Amendment) Regulations, 2026" for Consultation on 13th March 2026 to seek stakeholders' views on key regulatory amendments needed to strengthen the existing regulatory framework., enhance enforcement mechanisms and address emerging challenges in the prevention and regulation of UCC. The consultation focused on several vital issues, including leveraging AI/ML-based suspected UCC detection to aid in regulatory enforcement, strengthening mechanism for complaint-based action, expanding scope of explicit consent to accommodate legacy consents available with the entities, providing for appeal mechanism, strengthening the accountability of Senders and Telemarketers, regulating Application-to-Person (A2P) calls, strengthening safeguards against the misuse of Headers and Content Templates etc.

3. The comments and counter-comments on the draft regulations were received till 19th April, 2026, and 04th May, 2026, respectively. The Open House Discussion (OHD) with the stakeholders was held on 3rd June, 2026. After considering stakeholders' feedback and carrying out detailed analysis, the Authority has introduced the Telecom Commercial Communication Customer Preference (Third Amendment) Regulations, 2026 today.

4. SALIENT FEATURES OF THE AMENDMENTS

(i) Leveraging AI/ML-based suspected UCC detection to aid in regulatory enforcement

(a) Major Telecom Service Providers (TSPs) have already deployed AI/ML-based systems to detect suspected spam communications and alert the customers. The Authority also issued a

Direction on 27th February, 2026 to the TSPs for using AI/ML-based intelligence on suspected UCC for inter-operator sharing and to carry out further investigation of suspected UCC senders.

(b) The provisions of the said Direction have been suitably incorporated into the TCCCPR, 2018 through the introduction of Regulation 21A which mandates the TSPs to identify the sender's CLIs having a high probability of being used for sending UCC and share the information among the TSPs.

(c) Where five or more CLIs associated with a Sender are flagged within a period of ten days, further investigation and graded action will be initiated by the Access Providers, including KYC re-verification, physical verification, barring of outgoing services, and disconnection of telecom resource in cases of repeated violations and misuse of telecom resources.

(d) Special numbering series designated for commercial communications, including the 140xx, 1600xx and 1601xx series, shall not be flagged as suspected spam for recipients, thereby ensuring that legitimate commercial communications and government communications from the regulated series are not inadvertently missed.

(ii) Regulation of Application-to-Person (A2P) calls

(a) Application-to-Person (A2P) calling is being used for bulk commercial communications due to its ability to automate and scale large volumes of calls, and therefore, there exists a potential for their misuse for making spam calls.

(b) Accordingly, to regulate such calling, the amendments have defined A2P calls as voice calls initiated by an application, software system or automated platform without direct human dialing, including using autodialing, robo-calls and pre-recorded/artificial voice technologies. It has been mandated that every entity using A2P calls must pre-declare such use to its TSP along with the details of CLIs to be used for making such calls. A2P calls made without the required prior declaration will be treated as UCC.

(c) To act as a deterrent, a termination charge of up to ₹0.05 per minute has been introduced to be levied by the Terminating Access Provider on the Originating Access Provider for A2P calls.

(d) A2P calls made through any numbering series designated by the Authority for regulated commercial calls, and Authority-authorized calls are exempted from termination charges.

(iii) Commercial Communications based on inquiry:

(a) Commercial communications may be sent to a customer on the basis of an inquiry made by the customer to the sender for goods or products or services, only for a period of seven days from the date of such inquiry.

(b) However, to prevent the misuse of such provision for sending spam, it has been mandated that such an inquiry shall be made in writing or through digital means, and shall be maintained in a verifiable form by the Sender.

(c) The amendment is intended primarily to facilitate e-Commerce and e-Service Platforms.

(iv) Introduction of Consumer Appeal Mechanism

(a) Consumers will now be able to prefer an appeal against the resolution of UCC complaints. The appeal may be preferred within 15 days before the Appellate Authority.

(b) Appeals will be resolved by the Appellate Authority as per the Telecom Consumers Complaint Redressal (TCCR) Regulations, 2012.

(c) The appeal may be preferred through any of the modes available for lodging UCC complaints i.e. through TRAI DND App, TSPs App/Portal, and call or SMS to 1909 besides the modes specified under TCCRR, 2012.

(v) Strengthening of Complaint-Based Action against UCC

(a) The existing regulations provide a complaint threshold of 5 or more unique complaints within a period of ten days to trigger action against the UCC Sender.

(b) To enable early identification of UCC senders and faster action against them, the amendments have mandated corroboration of the complaint data received from consumers with the data of Senders detected by service provider's AI systems as suspected of sending UCC with high probability.

(c) Action will be triggered against the sender if there are 3 or more unique complaints within a period of ten days and the concerned Sender's CLI is also flagged by the AI/ML-based system as suspected of sending UCC.

(d) Certain timelines prescribed under the complaint mechanism have been revised keeping in view the practical time required for implementation.

(vi) Expanded Scope of Explicit Consent

The definition of consent has been expanded to include legacy consents already available with the entities. The framework is being amended to enable the recognition and digitization of such legacy consents. However, the legacy consents shall be considered valid only where they have been obtained through verifiable means and are subsequently registered on the Digital Platform of the TSPs.

(vii) Strengthening Measures against Misuse of Headers and Content Templates

(a) In cases involving misuse of Headers or Content Templates, the Originating Access Provider shall suspend the misused Headers or Content Templates, within six hours of becoming aware of such misuse, and issue a notice to the concerned Sender within the prescribed period.

(b) The concerned Sender shall be required to undertake specified remedial measures to prevent any further misuse, and file a complaint with the appropriate law enforcement agency. Where the misuse is attributed to a Telemarketer, all its telecom resources across the TSPs will be disconnected for a period of one year, along with blacklisting.

(viii) Essential conditions of Agreement between Access Providers and Senders/Telemarketers

(a) Under the regulatory framework, the TSPs have been obligated to ensure compliance of the regulatory provisions by the Senders and Telemarketer through contractual obligations between them. However, it has been observed that TSPs many times do not put strict conditions in the agreements to ensure compliance by these entities, primarily due to competition issues.

(b) Accordingly, to have more effective action against the Senders and Telemarketers engaged in sending UCC, a new provision has been introduced whereby the Authority may prescribe the essential conditions that must mandatorily form part of these agreements between the Access Providers and the Senders/ Telemarketers.

(ix) Classification of Senders

There exists a variety of Senders based on considerations such as the criticality of the services and the sector to which a Sender belongs, the importance of the entity to the economy, scale of operations, extent of usage of telecom resources by the Sender, and the potential impact of suspending/ disconnecting telecom resources of the Sender on the consumers. A new regulation has been introduced whereby the Authority may classify the Senders into different categories and may specify differentiated sets of enforcement measures applicable to such categories of Senders for violations of the regulations.

(x) Prohibition on blanket blocking/tagging by Call Management Applications

(a) Call Management Applications (CMAs) are prohibited from blanket blocking, filtering, or spam tagging calls from number series designated by the Authority or the Central Government for commercial communication such as 1600xx/1601xx for service and transactional calls, and 140xx for regulated promotional calls, since such tagging, without the safeguards built into the regulatory mechanism, risks mislabeling genuine commercial communications and government communications as spam, which are otherwise important to customers. However, individual consumers retain full freedom to block, or filter calls on their own devices.

(b) To facilitate wider collation of data for action against spammers, it has also been mandated that no CMA shall offer the users to report any unsolicited commercial communication under any name such as spam, junk, etc. on its platform, unless the CMA sends such report to the DLT platform maintained by the Access Providers.

(xi) Digital Interface for VNOs with the DLT Platform

As Virtual Network Operators (VNOs) are also Access Provider under the regulatory framework, the Network Service Operator (NSO) will be required to provide the VNO a digital interface having real-time functionality with the DLT platform and other systems necessary for the VNO to discharge its obligations as an Access Provider under the Regulations. This will address the operational difficulty presently being faced by the VNOs with respect to the access to the DLT Platform.

5. The amendments are aimed at strengthening consumer confidence in the commercial communication ecosystem, ensuring greater accountability across stakeholders, and enabling more effective and timely action against misuse of telecom resources by the spammers.

6. For further information, Shri Deepak Sharma, Advisor (QoS-II), TRAI, may be contacted at 011-20907760 or at email-id advqos@trai.gov.in

18/03/2026

(Harinder Kumar)
Secretary, TRAI