Fwd: Counter Comment in Consultation on Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

yashika.goplani < yashika.goplani@trai.gov.in >

rajesh Kumar < rk.vatsa73@trai.gov.in >

Mon, 04 May 2026 5:20:30 PM +0530

To "ASHOK KUMAR"<jtadv2-qos2@trai.gov.in>,"Sanjay Kumar"<jtadv-qos2@trai.gov.in>,"Jitender Yadav"<jitender.y@trai.gov.in>,"Yashika Goplani" <yashika.goplani@trai.gov.in>

Cc "advqos2"<advqos2@gmail.com>

========== Forwarded message ==========
From: Sircar, Indrajeet <isircar@amazon.com>
To: "advqos@trai.gov.in"<advqos@trai.gov.in>
Cc: "dait@trai.gov.in"<dait@trai.gov.in>
Date: Mon, 04 May 2026 16:58:01 +0530
Subject: Counter Comment in Consultation on Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026
========== Forwarded message ==========

Dear Sir,

I write on behalf of Amazon India. At the outset we thank the Telecom Regulatory Authority of India ("TRAI") for providing us with the opportunity of making our submissions on the Draft Telecom Commercial Communications Customer
Preference (Third Amendment) Regulations, 2026 ("Draft Regulations").

We note that the facility to submit counter-comments through the trai.gov.in portal has been disabled. However, in accordance with the revised timelines for submission of counter-comments (4 May 2026), and the guidance provided in the Consultation Paper dated 13 March 2026, we are hereby sharing our detailed counter-comments on the submissions received from various stakeholders on the Draft Regulations.

We remain available to address any queries or concerns you may have with the present submission.

Regards,

Indrajeet Sircar

Indrajeet Sircar
Manager, Public Policy
Mobile: +91. 8376037035| Email: isircar@amazon.com

amazon.com

work hard. have fun. make history.

---

1 Attachment(s)

Counter Comments from Amaz…
161.5 KB

Counter Comments on the Consultation on the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026.

We welcome the opportunity to make submissions on the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 ("**Proposed Amendment**") issued by the Telecom Regulatory Authority of India ("**Authority**")

In providing these counter comments, we have taken into account the existing regulatory framework under the Telecom Commercial Communications Customer Preference Regulations, 2018, as amended ("**Existing Regulations**").

We submit that certain aspects of the comments proposed by stakeholders as well as the Proposed Amendment may have unintended operational and compliance implications for legitimate enterprise communication and contact centre operations. Accordingly, the recommendations set out below seek to ensure that the regulatory objectives of consumer protection and traceability are achieved while maintaining proportionality, clarity of liability, and operational feasibility under the Existing Regulations.

A. Termination charges for Application-to-Person (A2P) calls (Regulation 35A)		
Proposed Amendment	**Issues/Submissions**	**Suggestions**
The Proposed Amendment introduces the concept of application to person (**A2P**) calls along with a requirement for prior declaration, failing which such calls may be treated as unsolicited commercial communication (**UCC**). It also proposes termination charges on A2P calls (currently at INR 0.05 per minute), as a deterrent to prevent the misuse of A2P calling for unregistered telemarketing. While calls originating from designated numbering resources such as the 140xx series (promotional) and 1600xx series (for specific regulated entities undertaking service and transactional communications) are outside the scope of this charge, A2P calls routed through regular numbering resources will attract A2P charges.	Certain stakeholders have welcomed the introduction of A2P termination charges and have further suggested removal of existing exemptions for designated numbering series such as 140xx and 1600xx, along with expansion of such charges across all commercial voice traffic. One stakeholder has also recommended increasing amount incurred for the termination charge to INR 0.50 per minute. However, these submissions appear to treat A2P calling as wrongful, whereas the regulatory intent is to curb unsolicited or non-compliant commercial communication. Hence, this approach does not adequately distinguish between non-compliant actors and legitimate enterprise communication, and risks imposing disproportionate burdens on compliant senders. Accordingly, expanding A2P termination charges or removing existing exemptions, as suggested by certain stakeholders, would disproportionately impact bona fide service and transactional communication, while not necessarily deterring unregistered or non-compliant actors who operate outside regulated frameworks. In fact, the scope of exemptions ought to be broadened rather than curtailed. A section of legitimate enterprise communication, particularly service and transactional calls by entities not covered under the 1600xx framework, continues to operate through regular numbering resources. There is no equivalent designated series available for such non-regulated entities	The Authority should not remove existing exemptions or expand A2P termination charges in a manner that captures legitimate service and transactional communications. Instead, the scope of exemptions should be broadened to include all bona fide service and transactional A2P calls, including those undertaken by entities not presently covered under designated numbering frameworks. In this regard, imposition of termination charges on A2P calls must be deferred until a complete and clearly defined numbering framework for all commercial communication is in place and all such numbering series must be excluded from the scope of A2P termination charges. Further, the Authority should bring service and

	undertaking service and transactional communications. Imposing termination charges on such traffic creates a significant cost burden on compliant businesses just because they use A2P technology for commercial communications and is a disproportionate measure to prevent the misuse of A2P calling by unregistered telemarketers.	transactional A2P calls across all sectors under the exemption provided for A2P termination charges.
B. AI/ML tracking for Unsolicited Commercial Communication (UCC) (Regulation 21A)		
Proposed Amendment	**Issues/Submissions**	**Suggestions**
The Proposed Amendment builds on the existing requirement for Telecom Service Providers (**TSPs**) to deploy AI/ML-based systems for detection of UCC but introduces additional trigger-based enforcement linked to such flagging under Regulation 21A. In particular, where 5 or more Calling Line Identities (**CLIs**) associated with a sender (*i.e.,* the entity sending or on whose behalf the commercial communication is sent) are flagged as "Suspected UCC CLI" within a 10-day period, the concerned Originating Access Provider (s) will be required to initiate graded action within prescribed timelines, consisting of re-verification of the sender's Know Your Customer (KYC) details.	Several stakeholders have supported the use of AI/ML-based systems as an important tool for detection of UCC and strengthening enforcement frameworks. While stakeholders have also raised concerns regarding the reliability of such systems when used as the sole trigger for enforcement action, some stakeholders have suggested enforcement actions such as disruption of services for cases with high confidence score through AI based solutions. Since the parameters used for AI/ML detection under the Proposed Amendment such as high call volumes, short call duration, and low incoming-to-outgoing ratios, are inherent to legitimate outbound contact centre operations, enforcement actions even with high confidence scores will not be feasible. While high confidence scores generated by AI-based spam detection systems may assist in prioritising or automatically filtering calls, they do not eliminate the need for human oversight. Such scores reflect probabilistic outputs rather than verified determinations and should be treated accordingly. This risk is particularly acute in UCC detection, where threat patterns are not static and spam callers continuously adapt their methods through number spoofing, CLI manipulation, and evolving social engineering scripts. Accordingly, outputs based on AI/ML measures, regardless of accuracy scores must be supported by human review to prevent creating a risk of adverse impact on lawful communications. The explanatory note to the Proposed Amendment (Explanatory Note) also recognises the need to minimise false positives and emphasises that such signals should be corroborated with additional evidence. This must be prescribed through measures for manual verification.	No enforcement action should be triggered solely on the basis of AI/ML based detection triggers without an additional layer of human validation. Alternately, any action pursuant to AI/ML based detection triggers must be coupled with actual complaints.

	Treating AI/ML outputs as determinative signals for enforcement actions, without adequate manual validation, may result in action against compliant entities. This can lead to disruption of business operations, and adverse impact on customer communication channels. Hence, requiring AI/ML detection to be verified through additional manual verification, and supporting evidence, ensures that actions are based on reliable and contextualised assessment rather than automated inference alone. This approach preserves the benefits of technology-enabled detection while ensuring that legitimate business communication is not adversely affected.	
C. Authority's power to designate classes of senders (Regulation 3(1) and Regulation 25)		
Proposed Amendment	**Issues/Submissions**	**Suggestions**
The Proposed Amendment introduces a framework empowering the Authority to classify senders into different categories and prescribe different compliance criteria and enforcement measures for each class.	We note that some stakeholders have suggested a removal of the proviso permitting sender classification for differential compliance and enforcement measures. We acknowledge the rationale for a differentiated or classification-based framework, particularly to account for varying use-cases and potential consumer impact. However, such classification must be grounded in clear, objective and transparent criteria to ensure consistency and predictability. The parameters for classification such as the importance to the economy, criticality of services, regulatory status, scale of operations, and potential consumer impact of suspension are subjective, and are not accompanied by any objective thresholds, procedural safeguards, or review mechanism. Such a classification creates an overly broad and discretionary power, with no embedded safeguards against arbitrary or inconsistent classification. In the absence of clear specific parameters, similarly placed entities may be treated differently without transparency or predictability, increasing compliance uncertainty. Such open-ended means for classification also weakens legal certainty, as entities would be unable to meaningfully anticipate the basis on which classification decisions will be made or how those criteria may evolve over time, and are therefore unable to structure or plan their commercial communications and business models.	The Authority's power to classify senders into categories, should be structured by clear, pre-defined, objective and reviewable criteria to ensure predictability, consistency, and to prevent arbitrary or inconsistent application. Any such framework should be issued only through a consultative direction, with prior publication of the proposed classification criteria and a reasonable period for stakeholders to consult.

	Accordingly, any sender-classification must be carried out only through a transparent, pre-published framework containing measurable criteria, reasoned determinations, opportunity for representation, periodic review, and an appeal mechanism against classification decisions.	
D. Disproportionate operational burden on senders (Regulation 22(1)(a))		
Proposed Amendment	**Issues/Submissions**	**Suggestions**
The Proposed Amendment revises the enforcement framework in cases of header/content template misuse by shifting from immediate suspension of all commercial communication traffic to a more proportionate approach focused initially on suspension of the specific misused headers or templates. At the same time, the proposed provision introduces detailed remedial obligations on the sender to be met within prescribed timelines failing which may result in suspension of all commercial communication by all TSPs. These include credential resets within 24 hours, filing complaints with law enforcement within 2 business days, de-registration and re-registration of headers/templates within 5 business days in certain cases, and a comprehensive review of all templates within 10 business days.	Some stakeholders have supported stricter accountability at the sender level, including through strong enforcement measures for systemic contraventions. However, such approaches do not fully account for the operational complexity involved in identifying the root cause of misuse, particularly in multi-layered enterprise and vendor-driven communication ecosystems. We welcome the move that removes the blanket suspension of all traffic to a more targeted approach focused on misused headers/templates, which reduces the risk of widespread disruption to legitimate commercial communication. That said, the associated remediation obligations and the relevant timelines are operationally challenging, particularly for large enterprises with multiple campaigns, templates, and vendor arrangements. Incidents of suspected misuse typically require internal investigation, coordination across teams and service providers, and technical validation before such remedial action can be taken. This creates a risk where entities may face escalation to suspension across TSPs despite acting in good faith to investigate and remediate the issue.	While retaining the approach to limiting suspension to only the misused headers and content templates, the Proposed Amendment should provide more realistic and proportionate timelines for compliance with remedial measures, taking into account the need for internal investigations and coordination. Accordingly, the Authority may consider introducing a staggered remediation framework, with initial containment measures followed by a reasonable period for full compliance, particularly where misuse appears limited or inadvertent. This may be supplemented by a de-flagging mechanism upon satisfactory compliance.