

Date; 19th April 2026.

To,
Sh. Deepak Sharma (Advisor-QoS-II),
Telecom Regulatory Authority of India (TRAI),
4th, 5th, 6th & 7th Floor, Tower-F,
World Trade Centre, Nauroji Nagar,
New Delhi: 110029

Subject: Submission of Stakeholder Comments on Draft TCCCPR (Third Amendment) Regulations, 2026 on behalf all the VNOs.

TRAI CP No. RG-25/ (25)/2023-QoS dated March 13, 2026 and Extension of last date of receive comments/ counter comments on the consultation dated 10-April-2026.

Dear Sir/Madam,

We write with reference to the Consultation Paper on the Draft Telecom Commercial Communications Customer Preference Regulations (TCCCPR) (Third Amendment), 2026, issued by the Telecom Regulatory Authority of India (TRAI).

At the outset, we appreciate the Authority's continued efforts to strengthen the regulatory framework governing commercial communications and to enhance consumer protection while promoting transparency and accountability across the ecosystem.

In this regard, please find enclosed herewith our detailed comments and suggestions on the draft amendments, prepared in accordance with the prescribed format (Annexure-I). Our submissions aim to ensure that the proposed regulatory framework remains practical with VNOs as Access providers Licensees for service delivery. VNOAI response is implementable, and aligned with current technological and operational realities, while effectively addressing the concerns of all VNO stakeholders.

We have endeavored to provide constructive feedback, along with detailed justifications, keeping in view the principles of proportionality, ease of compliance, and minimal disruption to existing systems and services.

We request the Authority to kindly consider our submissions while finalizing the amendments. We would be pleased to provide any further clarifications or participate in discussions, if required.

Thanking you,

Yours sincerely,
for **Virtual Network Operators Association of India (VNOAI)**



Rakesh Kumar Mehta
Secretary General
Mobile: +91 9899006599

Encl.: Annexure-I (Stakeholder (VNOAI) Comments on Draft Amendments).

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974

Regulation-wise Comments (TRAI Prescribed Format)

	Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
1	Regulation 2	new insertion - or clarify on existing clauses	<p>Request Adding the following proviso after the proposed definition of A2P calls:</p> <p>"Provided that a voice call shall not be classified as an A2P call if a live human agent is directly and actively participating as a party in the call at the time of connection, even if such call is initiated through an application programming interface (API), automated platform, or CPaaS system and using the same header / DID Number etc. Such calls shall be referred to as 'Human-Assisted API Calls' for the purposes of these regulations."</p>	<p>The proposed definition "initiated by an application, software system, or automated platform without direct human dialling" inadvertently captures human-assisted API calls (also known as click-to-call or agent-assisted calls) where a live human is connected as a party.</p> <p>These include:</p> <ul style="list-style-type: none"> • Ride-hailing driver-customer connections where the app connects a live driver to the customer. • Food / delivery coordination calls (delivery partner to customer). • Healthcare teleconsultation bridging (doctor to patient). • Enterprise customer support via agent dialer. <p>In all such cases, the API merely facilitates the connection — analogous to a telephone exchange. A live human is speaking on the call. These are not robo-calls or prerecorded messages. Subjecting them to A2P termination charges and the pre-declaration regime will impose enormous cost and compliance burden on legitimate transactional services without any UCC prevention benefit. A precise definition is essential before the charge and compliance regime is operationalized.</p>
2	New Regulation 21A(insered after Reg. 21)	All sub-regulations	<p>(a) Explicitly exclude Human-Assisted API Calls (as defined by the proposed provision in Regulation 2 (as mentioned above) from the scope of A2P termination charges.</p> <p>(b) Clarify the pre-declaration chain for VNO-mediated calls: the obligation to declare A2P usage should flow from the enterprise client to the licensed VNO, and from the VNO to the NSO — not directly from the enterprise client to the OAP/TAP, with whom VNO clients have no direct relationship.</p>	<p>(a) Human-in-loop API calls are not bulk automated communications. They do not exhibit the characteristics (automated, no live human, prerecorded/artificial voice) that the A2P deterrent regime is designed to address. Applying the same termination charge to a doctor calling a patient via a CPaaS / CCaaS platform as to a robo-call blasting thousands of numbers is both disproportionate and counterproductive.</p> <p>(b) VNOs (ULVNOs) are licensed intermediaries sitting between enterprise clients and NSOs/TSPs. An enterprise client registered on VNO's platform has no direct billing or contractual relationship with the OAP/TAP. The pre-declaration mechanism as proposed does not account for this intermediary layer. If the obligation is placed on the enterprise client to pre-declare to the OAP, compliance will be practically impossible for VNO-served entities. The mechanism must be redesigned to flow through the VNO.</p>

	Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
3	Regulation 25	Sub-regulation (5)(d)(i)	<p>(a) The reduced threshold of 3 unique complaints in 10 days (applicable when the CLI is AI-flagged as Suspected UCC CLI) should explicitly not apply where:</p> <ul style="list-style-type: none"> the CLI is assigned to a sender registered through a licensed VNO, AND the call/message is verifiably of transactional or service nature as per the DLT registration of the sender. <p>(b) Before triggering action at the reduced threshold, the OAP/TAP must verify the DLT registration status of the CLI and confirm whether the CLI belongs to a registered sender through a licensed VNO.</p> <p>(c) VNOs must be provided real-time visibility (via NSO) into AI-flagging of CLIs assigned to their enterprise clients, before any punitive action is initiated.</p> <p>(d) A mandatory notice-and-response window (minimum 2 business days) must be preserved even when the reduced threshold and AI flagging are both triggered, to allow the VNO and sender to present evidence of valid transactional use.</p>	<p>Complaint-based action against valid transactional use cases: Our experience across customers we find 80–85% of complaints are concentrated on top few high-volume customers whose use cases are validated transactional calls. Examples include:</p> <ul style="list-style-type: none"> Ride-hailing platforms: Driver calling customer to confirm pickup — customer marks it as spam due to service dissatisfaction. Food delivery platforms: Delivery partner calling to locate customer — customer reports the call while actually complaining about delayed delivery. E-commerce: Order confirmation and delivery update calls — reported as UCC when customers had not completed an order they changed their mind about. <p>These complaints, upon verification, are disposed as invalid. However, under the reduced threshold, punitive action (barring, disconnection) would be triggered before verification is complete, causing large-scale disruption to millions of end consumers.</p> <p>Risk of false AI flagging: Legitimate enterprise use cases — particularly click-to-call (where a single virtual number connects thousands of human-to-human calls) — exhibit volumetric patterns identical to UTM behavior (high call volume, same CLI). The AI system cannot distinguish a busy call center from a robe-call operation purely on volume metrics. Without the carve-out proposed, valid enterprise CLIs will be wrongly flagged.</p> <p>VNO blind spot: VNO don't have direct, real-time access and visibility to DLT complaint data or AI-flagging notifications. We learn of suspensions only through NSO notifications, by which time service disruption has already occurred. This need to be duly modified as suggested.</p>
4	Regulation 25	Sub-regulations (3), (4), (5) — timeline revisions	<p>Additional clarity required: The 5-business-day reply window should be for the sender from the time of intimation.</p> <p>For VNO-registered senders, the OAP notice must be simultaneously sent to the concerned VNO (through the</p>	<p>The timeline extensions are welcome. However, without the simultaneous VNO notification requirement, the 5-business-day window is not manageable for VNO-served enterprise clients: VNO (which manages the telecom resources) will not even be aware due to the current lack of transparent / seamless visibility to VNO in the NSO DLT.</p> <p>Timely VNO notification enables:</p>

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974

Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
		<p>NSO), so the VNO can investigate and seek clarity from the sender in sharing evidence submission.</p> <p>For VNO - customers VNO should be allowed to block, suspend and not the NSO - The NSO don't have the visibility of the client, use case and wrongly impact the enterprise customers.</p>	<p>(i) the VNO to investigate call records and investigate evidence of valid use;</p> <p>(ii) (ii) the enterprise client be informed and response is received; (iii) faster resolution with fewer wrongful suspensions as expected in framework's plans with overall objective of accuracy in complaint resolution can be met with this.</p>
5	Regulation 3	<p>First proviso to sub-regulation (1) [new enabling proviso]</p> <p>The enabling provision for classification of senders should explicitly:</p> <ul style="list-style-type: none"> Recognize licensed VNOs as a distinct category of intermediary within the sender classification framework. Enable TRAI to prescribe criteria for senders registered through licensed VNOs, including authorizing VNOs to represent their enterprise clients in regulatory proceedings and compliance submissions. Specify that suspension or disconnection of telecom resources of VNO-registered enterprise senders shall be coordinated with the concerned VNO directly. 	<p>The current regulatory framework creates a structural accountability gap: VNOs are held responsible for their clients' compliance but are not formally recognized as parties in enforcement proceedings. A sender registered through VNO platform interacts with TRAI's enforcement system through the NSO, with VNO invisible to the process.</p> <p>Formal recognition of VNOs in the sender classification framework would enable:</p> <p>(i) differentiated regulatory treatment for VNO-certified senders who have passed the VNO's own KYC and registration process;</p> <p>(ii) VNOs to be the first point of contact for compliance and enforcement, reducing the burden on OAPs/NSOs;</p> <p>(iii) more accurate attribution of UCC liability between the enterprise sender and the VNO intermediary.</p>
6	Regulation 8 and Regulation 22	<p>New sub-regulation (to be inserted)</p> <p>Insert a new provision under Regulation 8 or Regulation 22 mandating:</p> <ul style="list-style-type: none"> Every NSO shall provide its affiliated ULVNO licensees with real-time API-based access to: (i) UCC complaints received against telecom resources assigned to the VNO's 	<p>This is a foundational structural issue. VNOs are independently responsible for TCCCPR compliance as access provider but structurally lack the tools to fulfil this responsibility.</p> <p>The draft amendment adds significant new obligations (AI-triggered action at reduced threshold, CDR sharing with TRAI, enhanced complaint resolution timelines) without addressing the fundamental gap: VNOs have no direct DLT access and receive complaint/enforcement data only through NSOs, with unpredictable delays.</p>

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974

	Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
			<p>enterprise clients; (ii) AI-flagging alerts (Suspected UCC CLI notifications) for CLIs assigned to the VNO; (iii) CDR data relevant to complaint resolution for VNO-originated traffic.</p> <ul style="list-style-type: none"> The NSO shall route complaints against VNO-managed CLIs to the concerned VNO within two hours of receipt. NSOs shall implement DLT access model allowing VNOs to: independently onboard their Principal Entities; register headers and content templates; submit Action Taken Reports (ATRs); and access DLT compliance data — all within the NSO’s DLT node framework. Until such access infrastructure is fully operationalized, no VNO shall be penalized for failure to comply with complaint-handling or AI-response timelines it cannot independently observe. VNO enterprise clients should also be protected by regulator in similar lines. 	<p>As a result: (i) VNO cannot proactively monitor complaints against its enterprise clients’ CLIs; (ii) VNO has no visibility into which CLIs are being AI-flagged as “Suspected UCC CLI”; (iii) VNO cannot initiate corrective action before suspension is imposed; (iv) VNOI cannot independently file ATRs on behalf of clients.</p> <p>These obligations without access creates a framework that makes VNO compliance structurally impossible. The Authority must formalize the technical integration framework for VNO-NSO DLT access with binding timelines and SLAs, as part of this amendment itself.</p> <p>Till such time the authority should also protect VNO and VNO’s clients from any action from NSO - Which can potentially impact enterprises, sometimes impact essential services like doctor-patient calling, Gas booking etc handled by VNO and impact consumers / citizens. This is in spite of VNO and Enterprises are fully willing to comply with the regulations and are fully law-abiding entities.</p>
7	Regulation 34A	All sub-regulations	(a) Extend the prohibition on call management apps blocking, tagging, or filtering commercial communications to cover all calls from registered sender/telemarketer numbers — not just those using the 1600-series designated number range.	(a) The regulatory gap: The amendment protects 1600-series calls from app-based suppression. However, currently only BFSI entities have access to the 1600 series for outbound calls. Other enterprise clients in healthcare, logistics, e-commerce, and ride-hailing — who make equally valid transactional and service calls — use regular number series and remain fully exposed to OTT apps tagging their numbers as “spam” or blocking calls entirely.

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974

	Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
			(b) The requirement for call management apps to forward spam reports to OAP DLT platforms should explicitly include a parallel notification pathway to the VNO through whose platform the call was made, enabling the VNO to investigate and submit ATRs.	<p>An Uber driver calling a customer, a hospital calling with an appointment confirmation, or a logistics partner calling to arrange delivery should have the same protection from wrongful app-based suppression as a bank sending a transaction alert.</p> <p>(b) Without a VNO notification pathway, app-generated complaints will reach the DLT platform without the VNO's awareness, depriving the VNO of the opportunity to provide context and preventing accurate UCC attribution.</p>
8	Regulation 2	Clause (y) — being substituted (Explicit Consent)	<p>Support the revised definition of Explicit Consent that recognizes legacy consents lawfully obtained outside the CRF framework.</p> <p>Additionally propose: VNOs should be explicitly authorized to register legacy consents on behalf of their Principal Entity clients through the NSO-operated Consent Register Framework portal, using the VNO's unique Licensee ID and NSO provided access to DLT model.</p>	<p>Many of VNO's enterprise clients — particularly in BFSI, healthcare, and e-commerce — have large, lawfully-obtained offline consent databases that predate the CRF ecosystem. The revised definition rightly provides a pathway for recognizing and migrating these.</p> <p>However, without the ability for VNOs to upload legacy consents through their NSO DLT access, the migration process requires enterprise clients to interact directly with NSO DLT systems — an operationally complex and error-prone process. VNOs are best positioned to assist their enterprise clients in this migration, given their existing relationships and compliance frameworks. Formal authorization for VNOs to conduct consent migration on behalf of PEs is essential for orderly implementation.</p>
9	Regulation 3 + Schedule I	Enabling provision for sender classification & special number series	<p>(a) request TRAI to issue a time-bound roadmap (within 90 days of the amendment coming into force) for expanding the 1600 like-series designated number range to all sectors making legitimate transactional and service calls, including healthcare, logistics, ride-hailing, food delivery, and e-commerce.</p> <p>(b) Until the 1600-series is expanded, specify that: (i) AI-flagging and complaint-threshold mechanisms should give equal protection to registered senders in non-BFSI sectors making verified transactional calls; (ii) calls from registered senders</p>	<p>The current framework creates a two-tier system: BFSI entities enjoy the protection of dedicated 1600-series numbers for transactional and service calls, while equally legitimate transactional calls in healthcare, logistics, e-commerce, and ride-hailing have no such designation. This regulatory inequity has significant practical consequences:</p> <ul style="list-style-type: none"> • Non-BFSI transactional calls are exposed to AI-flagging because they originate from regular number series that are also used by UTM. • Call management apps freely suppress or tag non-1600 transactional calls as spam, with no regulatory prohibition. • The reduced complaint threshold (3 complaints) will disproportionately impact non-BFSI enterprise callers who lack the 1600-series protection. <p>The amendment's objectives of enabling legitimate commercial communication while curbing UCC cannot be achieved without closing this number-series gap. A time-bound roadmap for 1600-series expansion, with interim protections, is urgently needed.</p>

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974

	Regulation No.	Sub-regulation / Item	Modification Proposed to the Draft Amendment	Reasons / Full Justification for Proposed Modifications
			through licensed VNOs in transactional/service categories should not be subject to the reduced (3-complaint) threshold solely on the basis of being on non-1600-series numbers.	
10	Schedule I	Item 1(4) — verification and authentication methods	<p>We support the proposed enabling provision allowing the Authority to prescribe different/additional verification and authentication methods.</p> <p>Additionally propose: (a) TRAI should specify that licensed VNOs into cloud telephony, CPaaS and CCaaS who support large number of remote only working companies are allowed to serve using standards prescribed by the Authority; as alternatives to physical/biometric verification for enterprise senders registered through licensed VNOs. For eg. GST verification for address if the services are being served from cloud Telephony / CPaaS / CCaaS.</p>	<p>Physical verification and biometric authentication of companies in the current WFH and Remote working specifically when the service itself is being centrally delivered in a cloud / multi-tenanted model needs a differentiated view.</p> <p>This is consistent with broader government policy of encouraging digital KYC (Aadhaar e-KYC, Digi-Locker, CKYC) as equivalent to physical KYC for regulated entities. Things like GST verification can validate the authenticity of the company.</p>

Virtual Network Operators Association of India

Registered Office: 13th Floor, Room No. 1305,
Ambadeep Building,
14, K.G. Marg,
New Delhi – 110001.

Phone- 9899006599/9999917205

CIN No: U64200DL2016NPL304974