TTL Clause-wise Response on Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

S. No	Regulation No. /Provision	Sub Regulation/ Item No,	Modification proposed to the draft amendment	Reasons/full justification for the proposed modifications
(1)	**1. Short title, extent and commencement** These regulations may be called the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 (… of 2026).	(3) These shall come into force after ***thirty days*** from the date of their publication in the Official Gazette.	It should be at least 6 months in a phased manner from the date of their publication in the Official Gazette with due consideration of the suggested changes in the draft.	A 30-day implementation timeline is not practical, considering experience and the time required for i. process design, ii. resolution of operational complexities, iii. call centre/back-end team readiness, iv. DLT development, v. management of internal as well as industry-wide dependencies vi. time required for including non BFSI sector for service and transaction based calling through new series. 6 months are considering such action will be in place for fruitful implementation.
(2)	**2. Definitions - In these regulations, unless the context otherwise requires**	after clause (e) [1]the following clause shall be inserted, namely; *"(ea) An A2P (Application-to-Person) call refers to a voice call that is initiated by an application, software system, or automated platform without direct human dialling and delivered to an*	It can be used for having clear definition of A2P call (definition may be retained but the use for A2P may not be used for	1. Enterprises, BPOs, and call centres have been using dialers as an effective operational tool for past several years. They enable optimal utilization of telecom resources, improve efficiency, and support streamlined business

		individual telecom subscriber, including using autodialling, robo-calls and/ or prerecorded/ artificial voice technologies."	charging such calls) **Proposed definition -** *An A2P (Application-to-Person) call refers to a voice call that is initiated by an application, software system excluding the Service & transactional calls where human interaction is with customers, or automated platform without direct human dialing and delivered to an individual telecom subscriber, including using autodialing, robo-calls and/ or prerecorded/ artificial voice technologies."*	processes. 2. Agent-assisted calls should not be classified as A2P calls where auto-dialers are used only to reduce call setup and ringing time before connecting the call to a live agent. 3. Calls comprising purely pre-recorded messages may be classified as A2P (Application-to-Person) communications. Relevant use cases could include complaint callbacks, service notifications, and platform-mediated interactions such as connectivity between ride-hailing drivers, food delivery personnel, or healthcare tele-consultation providers and their customers, as seen in platforms like Amazon, Ola, Uber, Zomato, Swiggy, among others. 4. It is imperative that a clear, unambiguous definition of such A2P voice calls is established within the regulation. Leaving the interpretation open to PEs, TMs, or TSPs may lead to inconsistent implementation, ambiguity, and stakeholder dissatisfaction. 5. Such calls should not be subjected to termination charges, as there is currently no reliable technical mechanism to

				conclusively distinguish and validate whether a call is system-initiated (A2P) or agent-initiated, which may lead to disputes and incorrect billing. 6. These provisions should be made applicable only after the allocation of a dedicated numbering series for service and transactional communications across industries, ensuring proper identification, traceability, and regulatory compliance without impacting legitimate use cases.
(3)		for clause (y), the following clause shall be substituted, namely: - *"Explicit Consent" means such consent which has been either verified directly from the Recipient in a robust and verifiable manner and recorded by Consent Registrar; or, obtained by the sender through any verifiable means prior to or outside the Consent Registration Function framework and subsequently registered in the Consent Register in accordance with the procedure specified by the Authority."*	The proposed provision may be considered for bringing greater clarity to the definition of Explicit Consent. However, evidence shared by enterprises should continue to be treated as a valid and verifiable means of consent. It is requested that the provision be further elaborated until the CRF framework is fully functional.	1. The responsibility of TSPs should be limited to the implementation and operation of the CRF framework. 2. Consent should remain exclusively between the Principal Entity (PE) and the end user through the process prescribed by TRAI. 3. TSPs do not have the ability to independently verify or validate the authenticity of such consent. 4. Accordingly, accountability for obtaining, maintaining, and validating consent should rest solely with the Principal Entity and the end user.

(4)		in clause (ai), for the words "clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885)", ~~the clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885);~~ words "clause (g) of section 2 of The Telecommunications Act, 2023 (44 of 2023)", shall be substituted;		
(5)		for clause (ba), the following clause shall be substituted, namely:- ~~means specifically constructed experimental space, with a safe environment, within which various stakeholders can use Regulatory Technology solutions to develop and refine Code(s) of Practice to comply with new regulatory requirements;~~ "(ba) "Regulatory Sandbox" means a live testing environment where new products, services, processes, regulatory technology solutions and business models may be deployed for a limited set of eligible customers, for a specified period of time, with certain relaxations in the extant regulatory provisions in order to encourage and facilitate innovation		

		and technological development in telecommunication; development and refinement of Code(s) of Practice; and provide inputs for regulatory interventions and modifications."		
(6)		for clause (bb), the following clause shall be substituted, namely: - "(bb) "Relationship" means a prior or existing relationship (i) for business or commercial reasons, between a person or entity and a subscriber with or without an exchange of consideration, ~~ii. on the basis of the purchase or transaction made by or done by the recipient with the sender within the twelve months immediately preceding the date of the communication; or~~ (ii) on the basis of ~~inquiry or~~ application regarding products or services made by or submitted by recipient to sender within the **three months** immediately preceding the date of the receiving of communication, which relationship has not been~~(iv)~~	An inquiry may arise from an application or request submitted through web portals or other channels such as email, WhatsApp, or toll-free numbers. Such inquiries may be duly relied upon to establish that the recipient has expressed interest in availing the relevant product or service. Accordingly, "inquiry" should continue to be recognized within the prescribed timeframe for the purpose of establishing a relationship.	1. A period of 90 days from the date of the customer-initiated request may be considered valid. 2. Such period may serve as evidence of the customer's intent or consent to receive communications. 3. The communication should be limited to the specific product or service requested by the customer. 4. The regulation should clearly define the validity framework for customer consents across different scenarios and use cases. For instance: (a) Legacy consents may continue to remain valid until explicitly revoked by the customer, ensuring continuity of ongoing engagements; and (b) Prospective customer consents may be considered valid for a defined period (e.g., 3 months), beyond which they should lapse if not converted into an active customer relationship.

		~~for social reasons, between a person or entity and a subscriber with or without an exchange of consideration, by voluntary two-way communication, initiated from both sides at different points in time;~~		**5.** Such clarity will help ensure uniform interpretation, regulatory certainty, and better compliance across stakeholders.
(7)		in clause (bh), (i) its Customer or Subscriber to provide information pertaining to any product or service, its warranty, product recall, software upgrade alerts, safety or security of the product used or purchased by the Customer, periodic balance alerts, information regarding delivery of goods or services, and such messages or voice calls are not promotional in nature and do not require Explicit Consent; or (ii)a Recipient to facilitate or complete a commercial transaction involving the ongoing purchase or the use by the Recipient of the product or services offered by the Sender after obtaining Explicit Consent from the Recipient and such messages or voice calls are not promotional in nature:		

(8)		clause (bn), "Subscriber" means a person or legal entity who subscribes any service for telecommunication ~~to a telecom service provided by an Access Provider;~~		
(9)		clause (bo), "Telecom resources" means any ~~telegraph~~ telecommunication equipment and/or telecommunication identifier, as defined under The Telecommunications Act, 2023 (44 of 2023) used to send voice call or messages;		
(10)		clause (bw), "Unsolicited commercial communication or UCC" means any commercial communication that is neither as per the consent nor the registered preferences of the Recipient and does not include: - ~~Any transactional message or transactional voice call;~~		
(11)	3.: Commercial communications through network of Access Providers. —	(1) Every Access Provider shall ensure that any commercial communication using its network takes place only using registered headers or the resources allotted to	Classification may be considered by the Authority through the proposed Regulation Amendment for the	1. The definition of Registered Header should also include pre-declared headers/CLIs, in addition to designated number series. 2. There are sectoral entities beyond BFSI

		the Senders from special series assigned for the purpose of commercial communication. **"Provided that Authority may classify the senders for this purpose and may specify different criteria for different classes of senders."**	following sectors: • Healthcare and Pharmaceuticals • Telecommunications • E-commerce and Retail • Logistics and Supply Chain • Education and EdTech • Travel, Tourism and Hospitality • Real Estate and Housing Finance	that may require separate number series for business communications. 3. Based on the current implementation experience of the 1600XXX series in the BFSI segment, there have been significant operational disruptions. Key challenges include lack of incoming call functionality, decline in call connect ratios due to low customer familiarity with the new number series, and adverse impact on critical use cases such as collections—where intended recipients are either not answering calls or actively blocking these numbers, leading to reduced effectiveness. 4. In light of the above, entities may be allowed to continue using their existing UTM numbers, at least during the transition phase, to ensure business continuity and avoid disruption to ongoing operations. 5. Accordingly, provision for pre-declaration of existing number series and the purpose of communication on the DLT platform should be enabled. 6. This would support business continuity while ensuring regulatory compliance

(12)	4, Intimation regarding use of A2P calls ~~Auto Dialer or Robo Calls.~~ – Every Sender shall declare to ~~notify~~ the Originating Access Provider, in advance, about the use of Application-to-Person (A2P) calls. ~~Auto Dialer or Robo Calls as well as the intended objective of such calls in writing.~~ . Provided that any such call made by a sender without prior declaration to the OAP, shall be treated as unsolicited commercial communication (UCC), and the OAP shall take action against such sender as per the provisions of these regulations."		Clear guidelines are required for identification of A2P calls where no prior declaration exists, particularly for agent-assisted or AI-enabled interactions, to avoid ambiguity at the TSP level. Agent-assisted calls made through diallers with human intervention for genuine use cases such as service support, transactional updates, and customer-requested callbacks should not be classified as A2P calls or attract additional deterrent charges	1. There is need to clear the ambiguity as to how one can identify and prove that the call is made from A2P if it is not declared previously. There are humanoids which can be used or In case complaint was initiated against the agent-based call by calling it a A2P call It will be difficult at TSP end to identify such cases therefore some set of processes steps needs to avoid any ambiguity. 2. Agent based calls may not be considered as A2P where auto dialer is used 3. Agent-assisted calls initiated through dialler systems may not be classified as A2P communications for the purpose of applying additional deterrent charges. 4. In current enterprise operations, several legitimate communication use cases—including service calls, transactional updates, and customer-requested callbacks—are executed through auto-dialer systems, with or without human intervention. 5. In certain scenarios, AI/IVR-based bots initially handle the interaction, and where required, the call is seamlessly escalated to a live agent to ensure effective

				resolution and enhanced customer experience. 6. For instance, enterprises across sectors routinely use dialler-based systems to respond to customer requests—such as e-commerce platforms (e.g., Amazon, Flipkart), food delivery and logistics platforms (e.g., Zomato, Swiggy), mobility services (e.g., Ola, Uber), as well as banks and financial institutions and airline customer support teams for booking, service updates, and issue resolution. Accordingly, it may be appropriate to distinguish such agent-based communications from fully automated or bulk A2P calls, to ensure that genuine, customer-initiated engagement processes are not inadvertently subjected to additional operational and commercial/overheads or restrictions.
(13)	11. Every Access Provider shall give due publicity through appropriate means to make the customers aware regarding:	4. Every Access provider shall inform its Subscribers while giving telecom resources that he shall not get involved in the activity of sending Commercial Communication or cause sending Commercial communication, or authorize the sending of the		

		Commercial Communication using the telecom resources failing which the telecom resources used or assigned to him may be ~~put under Usage Cap or his telecom resources may be~~ disconnected;		
(14)	21A. For taking action against the senders suspected of sending unsolicited commercial communication, as detected by the AI/ML-based UCC_Detect system established by the access providers in accordance with Schedule IV, every access provider shall implement the following :-	(a) 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, and immediately upon such flagging and in any case within two hours of such flagging, share, through the Distributed Ledger Technology (DLT) platform, the flagged CLI with the concerned Originating Access Providers (OAPs);	Identification of CLI as suspected spam should exclude pre-declared numbers duly registered on the DLT platform. Since all enterprise communications may inherently meet behavioural calling pattern thresholds due to legitimate business operations.	1. The behavioural detection mechanism should be standardized across all TSPs to avoid inconsistent outcomes, customer dissatisfaction, and migration of traffic to unregulated OTT platforms such as WhatsApp. 2. A clear governance framework should be prescribed for detection logic and treatment of captive numbering resources vis-à-vis other TSP resources. It is suggested that implementation may initially focus on the retail subscriber base. 3. False positive cases must be explicitly addressed, considering the impact on customers, businesses, and brand reputation. 4. A formal review, remediation, and whitelisting mechanism should be introduced for suspected CLI cases to resolve ongoing challenges faced by

				enterprises and OAPs. 5. The regulation should formally notify Principal Entities (PEs) and Telemarketers (TMs) are that, based on their calling patterns, TSPs reserve the right to classify numbers as SPAM. 6. At the same time, the regulation must clearly define a proactive, standardized process for identifying and validating genuine use cases, rather than leaving such determinations solely to the discretion of individual TSPs. 7. Additionally, an escalation framework at the regulator level should be established to address situations where grievances raised by PEs and TMs are not adequately resolved by TSPs, ensuring transparency, accountability, and fair treatment across the ecosystem.
(15)		(b) upon receipt of the flagged CLI from the TAP, every OAP shall immediately issue a notification through SMS or mail or both, to the sender associated with such CLI, informing that based on communication behaviour, the CLI has been flagged as suspected		1. Upon notification that a sender's numbers have been marked as spam, the sender should be required to justify the relevant use case and calling pattern through a formal written submission. 2. Accountability for the sender's commitments should not rest with the TSPs. In cases where such customers are

		of sending UCC (spam)"; Provided that the authority may prescribe the format and manner of sending such notification from time to time.		subsequently found to be in violation, action may be taken in accordance with the applicable regulations. 3. A TRAI recommended (non TSP dependent) formal whitelisting mechanism should be introduced for validated customers, along with pre-declaration of CLIs (numbers) on the DLT platform to prevent unwarranted spam tagging. 4. Pre-declaration of existing resources, PRI, SIP, and other numbering resources on the DLT platform should be enabled. 5. In aggregator business models, where end-customer details may not be available with the OAP/TSP, mandatory pre-registration of sender CLIs on the DLT platform along with the communication purpose should be prescribed under the Regulation.
(16)		(c) OAP shall, within one business day of the receipt of the flagged CLI from TAP, identify unique KYC identifiers of the sender associated with such CLI, using its subscriber records, and share the same through DLT platform with		1. There is presently no visibility on the projected volumes of AI-based triggers, which is essential to assess the expected number of CLIs likely to be tagged at each OAP through the DLT platform. 2. Telecom resource allocation data for senders is often sourced from multiple

		all other Access Providers, who, within one business day of the receipt of such unique KYC identifiers from OAP, shall identify all the telecom resources allotted by them to such Sender;		internal systems such as CRM platforms. Accordingly, adequate implementation timelines are required for data collation, along with careful planning for manpower, complaint handling, and KYC processes. 3. In comparison to retail or individual users, enterprise customers are subject to significantly more stringent KYC and onboarding processes. In most cases, physical connectivity and infrastructure validation are established, and an authorized signatory—duly identified and verified—executes formal agreements and terms & conditions with the telecom operator. This ensures a higher degree of traceability, accountability, and compliance within enterprise communications. 4. For enterprise customers, such requirements may result in duplication of effort, as periodic physical inspections are already undertaken by TSPs as part of existing licence compliance obligations.
(17)		(d) upon identification of all the telecom resources allotted to such Sender, as referred in the preceding para, all the Access		**Same as above**

		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;		
(18)		(e) 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		1. The proposed requirement may lead to duplication of efforts and additional cost burden on TSPs. 2. Manual tracking of suspected UCC CLI data is likely to be highly voluminous and operationally intensive, making compliance within prescribed timelines impractical without timely system-driven inputs. Therefore, additional time for enterprise complaint handling is also requested to be discussed and formally agreed among PE, aggregators, VNO through the regulation. 3. A defined process should be introduced to address recurrence of legitimate cases

		follows: (i) 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 license conditions and take necessary action in accordance with the extant KYC guidelines. (ii) 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, outgoing services of all telecom resources including PRI/SIP trunks, SIMs etc. allotted to the sender shall be		impacted due to false positive identification.

		barred by all the Access Providers for a period of fifteen days, irrespective of whether those telecom resources were actually used or not in making such communications; (iii) 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.		

(19)	22 Other obligations of Access Providers	~~(i) ensure that traffic from the concerned Sender shall be suspended by all the Access Providers immediately till such time, the Sender files a complaint with the law enforcement agencies under the relevant laws, and Sender reviews all its Headers and Content Templates and takes corrective measures as per the regulations to prevent misuse of its Headers, Content Templates and other relevant credentials: Provided that no action shall be taken by Access Provider unless the concerned Sender has been given a reasonable opportunity of representation; (ii) ensure that, if Delivery TM is complicit in misuse of Headers or Content Templates, the Sender shall file a complaint against Delivery TM with the law enforcement agencies under relevant laws;~~		
(20)		(a) in case of misuse of Headers and/or Content Templates,		

(21)		(i) immediately suspend the use of such misused Header(s) and/or Content Template(s) across all Access Providers as the case may be, and the OAP shall issue a notice to the sender in whose name such Header(s) and/or Content Template(s) are registered, within 24 hours of reporting of misuse to the OAP. Such suspension shall remain in force until the conditions specified under sub-clause (ii) are fully complied with by the sender.		1. The proposed timeline may be revised to 24–48 hours. 2. In cases where the sender is not registered with the OAP, communication within shorter timelines may not be feasible due to the unavailability of contact details such as email ID or other registered coordinates.
(22)		(ii) require the sender to undertake all of the following remedial actions:		
(23)		1. Reset, within 24 hours of receipt of notice from the Originating Access Provider (OAP), all access credentials including passwords, API keys and system permissions used for submission or delivery of commercial communications, which have been allotted to the sender by the access providers and telemarketers;		

(24)		2. File a formal complaint with the appropriate law enforcement agency under the applicable laws, within 2 business days of receipt of notice from the OAP, clearly identifying whether the misuse arose due to— i. compromise of login credentials, ii. unauthorized access to systems, iii. misuse by an associated Telemarketer, Aggregator, or Delivery Entity, or iv. any other identifiable cause, to be specified by the sender; and share with the OAP a copy of the complaint filed. Provided that, if any Telemarketer is an accomplice in the misuse of Headers or Content Templates, the Sender shall file a complaint against such Telemarketer with the law enforcement agencies under relevant laws;		
		3. Where the Sender claims or the OAP determines that misuse occurred due to leakage, cloning, or compromise of credentials, the Sender, within next 5 business		

		days shall mandatorily de-register all its Headers and Content Templates including those reported as misused, and get them re-registered to obtain new header and template ids using the bulk tool provided by the concerned registrar access provider(s) to the sender for this purpose; and the sender shall ensure that previously compromised identifiers are not reused;		
(25)		4. (a) Conduct within 10 business days of receipt of notice from the OAP, a comprehensive review of all its registered Headers, Content Templates, Consent Templates; and (b) Intimate to the OAP whether the misuse was due to credential leakage, compromise of IT systems or any other reason, to be specified by the sender.		1. TSPs are not rule-making authorities and are often positioned merely as telecom service **Vendors**, despite being expected to enforce regulatory compliance. Therefore, it is essential that Telemarketers (TMs), Aggregators, and Principal Entities (PEs)—as key stakeholders in the communication ecosystem—are explicitly brought under the regulatory framework by TRAI, with clearly defined roles, responsibilities, and accountability mechanisms. 2. This approach will ensure balanced responsibility across all participants, rather than treating these entities merely as end users of telecom services and will

				lead to more effective and enforceable compliance outcomes. 3. It is possible that UCC may continue despite confirmations or undertakings from such entities; accordingly, TSPs should not be held solely responsible for the overall conduct of these stakeholders. 4. A standard agreement framework may be prescribed by the Authority for adoption across the ecosystem. 5. Registration of Telemarketers and Aggregators with TRAI should be mandated. 6. The responsibilities of Principal Entities (PE), Telemarketer Delivery (TD), and Telemarketer Aggregators (TA) should be explicitly defined, with direct penal consequences for any regulatory violations to ensure responsible participation and compliance.
(26)		iii. Where the Sender fails to fully comply with the obligations under sub-clause (ii) within the stipulated timeframe, or provides an incomplete or false intimation, all commercial communication traffic from such Sender shall be		

		suspended by all the Access Providers until compliance is achieved to the satisfaction of the OAP. Provided that the Authority may, from time to time, prescribe any other procedures, safeguards, timelines, and conditions to safeguard the security of the commercial communications.		
(27)	**23) Every Access Provider shall establish Customer Complaint Registration Facility (CCRF) and shall make necessary arrangements to facilitate its customers on 24 hours X 7 days basis throughout the year: -**	(1), (c) to appeal to the Appellate Authority within a period of 15 days from the date of receipt of information about the resolution of the complaint when the consumer is not satisfied with the redressal of the complaint by the Access provider, or the complaint remain unaddressed, or no intimation of redressal of the complaint is received by the complainant within a period of fifteen(15) days from the date of registering complaint, whichever is earlier. The complainant shall be able to prefer such appeal through any of the modes specified for lodging a complaint or report under these Regulations. The	~~1), (c) to appeal to the Appellate Authority within a period of 15 days from the date of receipt of information about the resolution of the complaint when the consumer is not satisfied with the redressal of the complaint by the Access provider, or the complaint remain unaddressed, or no intimation of redressal of the complaint is received by the complainant within a period of fifteen(15) days from the date of~~	1. It is submitted that a well-established and structured consumer grievance redressal mechanism is already in place for Telecom Service Providers (TSPs), which adequately covers complaints relating to Unsolicited Commercial Communications (UCC) as well. 2. The existing framework provides for complaint registration, tracking, resolution, and escalation, thereby ensuring that consumer grievances are addressed in a systematic and time-bound manner. 3. It is submitted that the proposed additional appellate layer may not necessarily result in improved effectiveness or outcomes in grievance redressal. On the contrary, the creation of

		Appellate Authority shall resolve and reply to such appeal within a period of fifteen (15) days from the date of its receipt. Every Access Provider shall designate a permanent employee working at senior management level as the Appellate Authority. The name and contact details of such designated officer shall be duly published at a prominent place on the official website of the concerned Access Provider."	~~registering complaint, whichever is earlier. The complainant shall be able to prefer such appeal through any of the modes specified for lodging a complaint or report under these Regulations. The Appellate Authority shall resolve and reply to such appeal within a period of fifteen (15) days from the date of its receipt. Every Access Provider shall designate a permanent employee working at senior management level as the Appellate Authority. The name and contact details of such designated officer shall be duly published at a prominent place on the official website of the concerned Access Provider."~~	a parallel appellate mechanism specifically for UCC complaints, separate from the existing framework, may lead to duplication of processes without delivering commensurate benefits to consumers. 4. The requirement for each Access Provider to designate a senior management-level Appellate Authority, along with associated infrastructure and processes, would impose significant administrative, burden on TSPs, restructuring of internal processes, and ongoing compliance costs, which may not be as per intended outcomes. Thus, the existing consumer grievance redressal and escalation mechanisms may continue to be leveraged for handling UCC-related complaints; and introduction of a separate, dedicated appellate mechanism under these Regulations may be reconsidered.
(28)		~~(i) to record three years~~		

	24Distributed Ledger(s) for Complaints: Every Access Provider shall establish or cause to establish Distributed Ledger(s) for Complaints (DL-Complaints) with requisite functions, processes and interfaces:	~~history of complainant with details of all complaint(s) made by him, with date(s) and time(s), and status of resolution of complaints;~~		
(29)		"(3) to record three years' history, complainant-wise, with details of all complaints including appeal, if any and alleged violations reported by the complainants, with date and time, and status of resolution of complaints including the supporting documents used by the access providers for resolving the complaints;"	**"to record one year" history**	1. With the continuous increase in complaint volumes, maintaining records for a period of three years has become increasingly challenging due to significant storage requirements. 2. A substantial portion of the retained artifacts relates not to customer evidence, but to internal correspondence concerning the handling of UCC complaints through email communications. 3. Such emails are typically archived over time, and retrieval beyond one year becomes operationally difficult, time-consuming, and inefficient despite considerable effort. 4. In view of these operational constraints and scalability challenges, it is respectfully requested that TRAI reconsider the existing requirement and permit a reduced record retention period

				of one year for UCC complaints.
(30)		4) to record three years history of sender(s) against which complaint including appeal, if any is made or reported with details of all complaint(s) including appeal, if any, with date(s) and time(s), and status of resolution of complaints;		**Same as above**
(31)	25. Complaint Mechanism: Every Access Provider shall establish systems, functions and processes to resolve complaints made by the Customers; corroborate the complaint data with the data of senders suspected of sending UCC by the AI/ML based UCC detect systems across all the access providers,; and ~~to~~ take remedial action against Senders as provided hereunder (Sender herein shall mean a sender or telemarketer, who has been allotted the telecom resource by the access provider, that has been used for making such communication, and against			
(32)		the Terminating Access Provider shall also verify if the date of receipt of complaint is within seven days of receiving Commercial Communication and in case the complaint is reported by the Customer after seven days, it shall communicate to the Customer about the closure of his complaint along with reasons in accordance with the Codes of Practice for Complaint Handling and change status of the complaint on DL-Complaint as a report instead of a complaint: Provided that the Authority may, if it so desires, by		1. This would be operational overhead for OAP may be managed at TAP end. 2. Frequent regulatory changes necessitate corresponding modifications to the DLT platform, which is presently undergoing multiple concurrent developments. 3. In view of the associated operational complexities, it is requested that the complaint registration timeline continue to remain within 7 days from the date of receipt of the complaint. Extending this timeline may lead to inaccuracies in the details provided by complainants, particularly in the case of voice communications, where recall of header or originating details tends to diminish

	which the UCC complaint has been made.):-	direction, specify the content and method of making such communication to the complainant; Provided further that every complaint reported by the customers after seven days but before the lapse of fifteen days of the receipt of the unsolicited commercial communication by the customers, shall be recorded by the terminating access provider as well as the originating access providers;		over time. This increases the risk of incorrect identification of the Principal Entity (PE), thereby subjecting unrelated entities to unnecessary investigation and compliance burden. 4. Maintaining the 7-day window will help ensure data accuracy, fair attribution, and efficient resolution of complaints. 5. This is particularly important in the case of enterprise customers, for whom a separate complaint handling process has already been proposed.
(33)		4 b) examine communication detail records, within ~~one~~ two business days from the date of receipt of compliant by OAP to check the occurrence of complained communication between the complainant and the reported telephone number or Header from which Unsolicited Commercial Communication was received;		
(34)		4 d) in case of occurrence of SMS-related complained communications under sub-regulation (4)(b), OAP shall further		

		examine, within ~~one~~ three business days from the date of receipt of complaint by the OAP, whether all regulatory pre-checks were carried out in the reported case before delivering Unsolicited Commercial Communications; and		
(35)		4 d (ii) in case of non-compliance with the regulations, within two three business days from the date of receipt of complaint by the OAP, take action against the defaulting entity and communicate to TAP to inform the complainant about the action taken against ~~his~~ the complaint as provided for in these regulations and Codes of Practice: Provided that the Authority may, if it so desires, by direction, specify the content and method of making such communication to the complainant; Provided also that in case of complaint originating due to registration of content template in wrong category, the content template shall be blacklisted by the OAP; and if five content templates of such sender are blacklisted for		

		registration under wrong category, the OAP shall suspend the services of the sender, for one month or till such time all the content templates of the sender are reverified for registration under proper category, whichever is later;		
		e) in case of occurrence of complained communication related to Voice Call from the series assigned for promotional call under sub-regulation (4)(b), further examine, within ~~one~~ three business days from the date of receipt of complaint by the OAP, whether all regulatory pre-checks were carried out in the reported case before delivering Unsolicited Commercial Communications; a		
(36)		e(ii) in case of non-compliance with the regulations, within two three business days from the date of receipt of complaint by the OAP, take action against the defaulting entity and communicate to TAP to inform the complainant about the action taken against his complaint as provided for in the Regulations		

		and Code(s) of Practice:		
(37)		f) in case of occurrence of complained communications under clause (4)(b) related to promotional Voice Calls made using the number resource(s) allotted from series assigned for transactional and service calls, further examine within a maximum time of ~~two business hours~~ one business day, whether there are similar complaints or reports against the same Sender;		
(38)		i) ~~if it is found that the number of complaints against the Sender are from five or more than five unique Recipients during the last ten days,~~ if it is found that there are five or more complaints against the sender from unique recipients during the last ten days, immediately suspend the outgoing services of all the telecom resources of the sender which were utilized for sending UCC and simultaneously initiate	**"if it is found that there are Fifty Valid complaints against the sender from unique recipients during the last Fifteen days"**	1. A differentiated approach should be considered for complaint handling in the case of enterprise senders vis-à-vis individual or retail mobile subscribers. 2. Given that enterprises manage large customer bases, their communication patterns are inherently high-volume and business-critical. Accordingly, applying a uniform threshold of five complaints within ten days may not adequately reflect the operational scale and context of enterprise communications, and could lead to disproportionate outcomes.

		investigation by issuing a notice to the sender, under ~~sub-regulation (5)(d)(i)~~ to give opportunity to the sender to represent the its case within five business days; thereafter investigate within five business days from the date of receipt of representation from the sender or expiry of the five business days period given to sender for representing the case, whichever is earlier, and record the reasons of its findings. and if the conclusion of the OAP is that the sender was engaged in sending the Unsolicited Commercial Communications, it shall act against such sender as under		3. Furthermore, in a majority of enterprise scenarios, 95–98% of complaints are customer-perceived, often resulting in false positives. Therefore, immediate suspension of telecom resources upon the threshold being triggered at the first instance may be unduly disruptive and could adversely impact critical customer-facing services and business continuity. 4. It is recommended that enterprises be provided a fair notice period of at least seven business days to review the complaint and justify the communication intent before any restrictive action is initiated as lot of enterprises are relying on the service experts like BPOs and intent clarification for such intermediaries from PEs is a time consuming process 5. The framework may incorporate calibrated thresholds and contextual evaluation criteria for enterprises, taking into account factors such as scale of operations, nature of services, and existing customer relationships. This would help prevent disruption of legitimate business communications

				while continuing to address misuse effectively. Illustrative sectors may include e-commerce, logistics, mobility, and other customer service platforms such as Amazon, Flipkart, Swiggy, DHL, Ola, Health care etc. 6. A graded four-step enforcement framework for enterprises may be considered as under: **First Violation:** Warning **Second Violation:** Barring for 5 days at OAP level **Third Violation:** Barring for 15 days across all TSPs **Fourth Violation:** Blacklisting for 1 year
(39)		~~Provided further that the Authority may specify different criteria for initiating action under sub-clauses (i) and (ii) above from time~~ to time; Provided further that the Authority may, from time to time, classify senders into different categories based on the parameters including, but not limited to,— (a) the importance of the entity to the		1. A differentiated complaint management framework is required, including a separate complaint handling process for enterprise customers. 2. Additional timelines for action on complaints should be considered in enterprise scenarios, as large-scale operations and the requirement to obtain evidence from end customers involve greater complexity compared to the retail segment.

		economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/ disconnection of telecom resources on consumers; and may, accordingly, specify differentiated criteria for initiation of action and differentiated sets of enforcement measures applicable to such categories of Senders for violations of these regulations.		3. The process and minimum evidentiary criteria to be accepted by TSPs should be clearly prescribed for different sectors such as Banking, E-commerce, and other industries. 4. Call recording requirements may be considered mandatory for sectors such as E-commerce and other relevant industries, while the Banking sector may continue under its existing sector-specific regulatory provisions. 5. A separate category for Aggregators should be introduced, considering that they service multiple end-user entities and operate under a distinct business model. 6. Any entity providing support services to enterprises—whether through **manpower, technology platforms, or end-to-end solutions (including telecom resources)**—should be **explicitly covered within the regulatory framework through dedicated provisions**. 7. These provisions must include **clearly defined roles, responsibilities, and accountability mechanisms**, enabling **appropriate and enforceable action in the event of any violations**

				8. Declaration of all telecom resources / UTM numbers on the DLT platform, along with the purpose of communication, should be mandated to prevent unwarranted spam tagging of genuine enterprise users.
(40)		5 b) OAP shall examine communication detail records (CDRs), within ~~one~~ two business days from the date of receipt of compliant ~~complaint~~ by OAP, to check the occurrence of complained communication between the complainant and the reported telephone number from which Unsolicited Commercial Communication was received;		
(41)		5 d) in case of occurrence of complained communications under sub-regulation ~~clause~~ (5)(b), OAP shall further examine within a maximum time of ~~two business hours~~ further one business day, ~~whether there are similar complaints or reports against the same Sender; and (i) if it is found that number of complaints against~~		

		~~the Sender are from five or more than five unique Recipients during last ten days, OAP shall suspend the outgoing services of all the telecom resources of the Sender irrespective of whether those telecom resources were actually used or not in making such communications and initiate an investigation as provided for in the sub-regulation (6);~~		
(42)		5di) if it is found that there are three or more complaints against the sender from unique recipients during the last ten days, and also any CLI allotted to the sender has been flagged or maintained as "Suspected UCC CLI" by the AI system of the access providers during these last ten days, OR, if there are five or more complaints against the sender from unique recipients during the last ten days, the OAP shall immediately suspend the outgoing services of the telecom resources of the Sender which were utilized for sending UCC and simultaneously initiate an investigation as provided for in the		1. The parameters for marking a CLI as spam should be clearly defined in the Regulation and uniformly shared with all TSPs. 2. The logic for identification of suspected CLIs should be standardized across all TSPs, supported by a clear audit and governance mechanism to ensure consistent implementation. 3. A separate complaint handling framework should be prescribed for enterprise service providers, as the proposed amendment may result in a higher incidence of false positives and additional compliance burden on TSPs. 4. As an interim approach, action may be considered only where the same CLI is

		sub-regulation (6);		consistently identified as suspected across multiple TSPs and supported by valid complaint data. 5. Enterprise communication patterns, particularly in sectors such as BPOs, Aggregators, and BFSI, are inherently high-volume and may therefore require contextual evaluation before any restrictive action is taken. 6. It is recommended that Phase I of the implementation be initiated with a pilot focused on SIM-based solutions, where controls and enforcement mechanisms can be operationalized immediately with minimal complexity and large scale disruptions. This approach will enable faster rollout, controlled testing, and early identification of implementation challenges. 7. Based on the learnings and outcomes from the pilot phase, the framework may subsequently be extended to the enterprise segment. This expansion should be undertaken post allocation of dedicated numbering series for service and transactional communications, or by leveraging existing resources/headers

				already declared on the DLT platform, ensuring continuity, compliance, and minimal disruption to legitimate enterprise communications. 8. A transparent and standardized operating framework should be adopted with adequate visibility to OAPs in order to reduce ambiguity and ensure uniform implementation. 9. A graded four-step enforcement mechanism may be considered for enterprise cases involving genuine use-case scenarios, as under: First Violation: Warning Second Violation: Barring for 5 days at OAP Third Violation: Barring for 15 days across TSPs Fourth Violation: Blacklisting for 1 year 10. In cases where action is triggered due to potential false positives, a provision for immediate review, remediation, and restoration of services upon validation by the enterprise should be introduced. 11. Such safeguards are essential to prevent disruption of legitimate business operations and customer-facing services.

(43)		5d(ii) in case, it is found that number of complaints against the sender are from less than five unique recipients during last ten days, OAP shall communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner specified in the Codes of Practice: and none of the CLIs of the sender has been flagged or maintained as "Suspected UCC CLI" by the AI system of the access providers during these last ten days, the OAP shall communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner specified in the Codes of Practice. Provided that the Authority may, if it so desires, by direction, specify the content and method of making such communication to the complainant: Provided further that the Authority may, from time to time, classify senders into different categories and specify differentiated criteria for initiation of action against them		1. As suggested, parameters such as the importance of the sender, level of criticality, communication volumes, and telecom resources deployed may involve subjective assessment. Any action or non-action taken on this basis may also have legal implications for the TSP. 2. In cases where an entity has a limited number of telecom resources and actions such as disconnection or blacklisting are initiated, such measures may be undertaken at the industry level without prior information to, or visibility of, the regulator. Accordingly, it is essential that any pre-declared exemptions for such senders be formally shared by the Authority to enable appropriate action planning at the TSP end. 3. While the existing provision enables classification of senders and differentiated treatment based on defined parameters, it is important that this distinction be explicitly operationalized for enterprise use cases. 4. Enterprises operate at substantially different operational and commercial scales as compared to individual senders

		under sub-clauses (i) and (ii) above, based on the parameters including, but not limited to (a) the importance of the entity to the economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/ disconnection of telecom resources on consumers;		or entities relying on retail SIM-based communications. Their communication frameworks are often critical for customer service delivery, transactional messaging, and essential business operations across sectors such as BFSI, e-commerce, logistics, healthcare, and other key industries. 5. In view of the above, it is recommended that enterprises be proactively identified as a separate category, supported by clearly defined and differentiated thresholds, evaluation criteria, and enforcement mechanisms. 6. Applying uniform thresholds designed for retail or small-scale senders may not adequately reflect the scale, nature, and intent of enterprise communications. 7. Recognizing enterprise communications as an important enabler of economic activity, a calibrated and differentiated regulatory framework would help achieve an appropriate balance between consumer protection objectives, business continuity, and service reliability.

(44)		in case of occurrence of complained communications under sub regulations (5)(d)(i) above, OAP shall, immediately issue a notice to the sender to give opportunity to represent the case its case within five business days; thereafter, shall investigate within five business days from the date of receipt of representation from the sender or expiry of the five business days period given to sender for representing the case, whichever is earlier, and record the reasons of its findings and. If the conclusion of OAP is that the sender or its TM was engaged in sending the Unsolicited Commercial Communications, OAP shall take action against such sender as under-		
(45)		for the first instance of violation, outgoing services of all telecom resources allotted to the Sender including PRI/SIP trunks, SIMs etc. allotted to the sender shall be barred by all the Access Providers for a period of fifteen days, irrespective of whether those		1. It is recommended that enterprises be proactively recognized as a distinct category, with clearly defined and differentiated thresholds, evaluation criteria, and enforcement mechanisms. Recognizing enterprise communications as a key enabler of economic activity, a calibrated and differentiated regulatory

		telecom resources were actually used or not in making such communications; (b) for the second and subsequent instances of violations, - (i) all telecom resources of the Sender including PRI/SIP trunks, SIMs etc. of the sender shall be disconnected by all the Access Providers for one year, irrespective of whether those telecom resources were actually used or not in making such communications; (ii) OAP shall put the Sender under the blacklist category during the period of one year as above and no new telecom resources shall be provided by any Access Provider to such Sender during this period;		approach would help balance consumer protection objectives with the need to ensure business continuity and service reliability. 2. Accordingly, the complaint handling process applicable to enterprise communications requires careful examination and suitable customization in view of the unique nature and scale of enterprise operations. 3. Considering that 95–98% of complaints are customer-perceived, often resulting in false positives, the immediate barring of telecom resources upon the threshold being met at the first instance may be highly disruptive for enterprises and could adversely impact critical customer-facing operations. 4. It is therefore recommended that enterprises be provided with a minimum notice period of at least seven business days to review, validate, and justify the communication intent before any restrictive or punitive action is initiated. as lot of enterprises are relying on the service experts like BPOs and intent clarification for such intermediaries from

				PEs is a time-consuming process. 5. The framework may incorporate calibrated thresholds and contextual evaluation criteria for enterprises, taking into account factors such as scale of operations, nature of services, customer dependency, and existing customer relationships. This would help ensure that legitimate business communications are not inadvertently disrupted, while continuing to effectively address instances of misuse. 6. For the enterprise segment, particularly in cases involving genuine use-case scenarios, a progressive four-step enforcement process may be considered, as under: First Violation: Warning Second Violation: Barring for 5 days at OAP Third Violation: Barring for 15 days across TSPs Fourth Violation: Blacklisting for 1 year
(46)		b iii) Provided further that the Authority may, from time to time, classify senders into different categories based on the parameters		Same as above

		including, but not limited to,— (a) the importance of the entity to the economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/ disconnection of telecom resources on consumers; and may, accordingly, specify differentiated criteria for initiation of action and differentiated sets of enforcement measures applicable to such categories of senders for violations of these regulations.		
(47)	26	2A Every access provider shall maintain, record of every alleged violation of the regulations, reported by its customers within fifteen days of the receipt of the unsolicited commercial communication by the customers, and shall also record reports of such alleged violations of the regulations		

		received from the other terminating access providers.		
(48)		4A) For the purpose of audit of complaint handling process, the terminating and originating access providers shall provide the requested CDRs of the relevant period to the Authority.		
(48)	27 Consequences for failure to take action against curb the Unsolicited Commercial Communications from registered Senders or RTMs – (1) If an Access Provider fails to ~~curb Unsolicited Commercial Communications~~ to take action in accordance with the provisions of the 'Regulations' against Unsolicited Commercial Communications from registered Senders or RTMs, the Authority may impose financial disincentives on such Access Providers in each Licensed Service Area for each calendar month as under:			
(49)		27 a) without prejudice to any penalty which may be imposed under its licence or under any Act for the time being in force, OAP shall be liable to pay, by way of financial disincentive, an amount of one thousand rupees per count of valid complaint that is declared invalid: Provided that where UCC has originated due to Headers ~~and Content Templates~~ registered by another Access Provider in violation of the regulation thereon and OAP has taken action against such UCC as per regulation of these regulations, the financial disincentive at the rate of one		1. TSPs are not rule-making authorities and are often positioned merely as telecom service **Vendors**, despite being expected to enforce regulatory compliance. In this context, it is essential that the Authority brings all key stakeholders within the ambit of the UCC regulatory framework, so that compliance obligations are equitably distributed and do not remain confined solely to TSPs, whose role is primarily that of telecom infrastructure providers. 2. Such an approach will ensure shared accountability, balanced enforcement, and more effective regulatory outcomes across the ecosystem. 3. Implementation of the CRF framework is

		thousand rupees per count of valid complaint ~~as above~~ shall be imposed on the Access Provider that has registered such Headers. ~~and Content Templates, instead of OAP~~ Provided further that where UCC has originated due to (i) wrong categorisation of Content Templates registered by the OAP, or, (ii) Content Templates registered under wrong category by another access provider and the traffic has been sent by the OAP under the wrong category, the financial disincentive shall be imposed at the rate of one thousand rupees per count of valid complaint on the OAP as well as the access provider that has registered such Content Templates under wrong category.		expected to improve complaint resolution efficiency, as the current process of gathering evidence is time-consuming and operationally intensive. 4. Penalty provisions may be limited to cases of incorrect registration or categorisation of templates, which should be the primary basis for imposition of financial disincentives. Clause like TCCCP 2010 for additional security deposit may be mandated through the Amendment Regulation for considered in case of repeated complaints from PE. a. Upon issuance of the first complaint notices by the Access Provider for unsolicited commercial communication, the Second Party shall deposit an additional security amount of Rs. 1,00,000/-. b. Upon issuance of the second violation notice for similar unsolicited commercial communication, the Second Party shall deposit an additional security amount of Rs. 1,50,000/-. c. Upon issuance of the third violation notice for similar unsolicited commercial communication, the Second Party shall deposit an additional security amount of Rs. 4,00,000/-. d. In case of violation the earlier deposited security deposit will be forfeited.

				Such payments to be deposited to the authorities and may be corroborated with the PMRs of the respective months. It is another way of bringing stakeholders in the regulation, across telcos with due audit mechanism by the Authority
(50)	29) Representation by Senders or Telemarketers against the action taken by Access Providers.— (1) The Authority may on receipt of a complaint from the sender or telemarketer, within sixty days of action taken against it by the Access Provider under the regulations 25, if it considers expedient to do so, call for the relevant details from the sender or telemarketer and Access Providers, and upon examination, for reasons to be recorded,			
(51)		if the Authority finds that conclusion of investigation by the Access Provider lacks adequate evidence against the sender or telemarketer, - (i) it may direct the Access Providers to restore all telecom resources of the sender or telemarketer and delete the name and address of such sender or telemarketer from the blacklist; (ii) may issue warning to the Access Provider for not exercising due diligence in deciding such cases Provided that while the sender or telemarketer may apply to the Authority for partial restoration of the telecom resources and removing the sender or telemarketer from the blacklist, the restoration charges		1. While the provision enables restoration of telecom resources in cases where investigations lack adequate evidence, a clearly defined and time-bound process should be prescribed by the Authority for handling such cases. 2. In the absence of defined timelines and procedural clarity, Principal Entities (PEs) and Telemarketers (TMs) may continue to approach Access Providers for resolution, resulting in operational inefficiencies and uncertainty. 3. It is therefore recommended that a structured workflow be established with defined timelines for review, decision-making, and restoration to ensure predictability, timely resolution, and accountability across stakeholders. 4. The Authority should also prescribe clear procedures for closure of complaints

		payable by the sender or telemarketer shall not be less than half of the restoration charges calculated to restore all the telecom resources of the sender or telemarketer.		arising from false positives. 5. A formal whitelisting mechanism for CLIs should be introduced to prevent recurrence of unwarranted actions against legitimate communications.
(52)	34 A) Prohibition on blocking designated number series by Call Management Applications.— (1) No call management application or similar services for identification of UCC shall tag, block, filter, give any treatment to such calls different from those applicable for genuine communication or restrict incoming calls ~~or messages~~ originating from any the designated number ~~series designated~~ for commercial communications, ~~as well as communication sent by the Government,~~ or facilitate blanket blocking of such communications as spam; (2) ~~Any Call~~			
(53)		(2) Any call management app including phone dialers and third party apps, that offers the user of the app to report any Unsolicited Commercial Communication under any name such as spam, junk, etc., which implies UCC, shall send such report, in the manner and format as specified by the Authority from time to time to the DND registry maintained by the access providers. Provided that the Authority may prescribe the manner of sending such complaints by the call management apps to the DND registry maintained by the access providers.		

(54)	~~Management Application that facilitates blanket blocking of such designated number series or tag it as spam shall be deemed non-compliant with these regulations: Provided that the consumers shall have the right to individually manage their own call through such Call Management Applications: Provided further that Authority may take appropriate enforcement measures, against non-compliant Call Management Applications in coordination with relevant authorities, if required~~.	3) Any call management application or similar services that act in contravention of sub-regulation (1) and (2) shall be deemed to be non-compliant and in violation of these regulations;		
(55)		(4) The Authority may order/initiate action against any non-compliant call management application or similar service as follows: (i) The Authority may issue warning for the violations, and declare call management application or the service as non-compliant and violator; (ii) The Authority may initiate action under the relevant provisions of the IT Act, 2000, and the IT Rules, 2021, for the violation of the regulations. If the authority concludes that the call management application or similar service is non-compliant, the IT intermediary shall be liable for losing exemption from liability of intermediary under IT Act 2000, and any other action as per the provisions of the IT Act, 2000. Provided that no order for action/		1. Timely and effective action against such entities is essential, as prolonged inaction has enabled them to continue operations that adversely impact the reputation and trust of legitimate enterprises. 2. At present, no defined mechanism exists for coordination with or reporting to the concerned Ministry. It is respectfully requested that the Authority establish a formal process for reporting, inter-agency coordination, and time-bound enforcement action.

		initiating action shall be made by the Authority, unless the concerned entity has been given a reasonable opportunity to represent		
(56)		35 i) any message transmitted by or on behalf ~~the directions~~ of the Central Government or State		
(57)		35 ii) any message transmitted by or on behalf ~~the directions~~ of bodies established under the Constitution;		
(58)	35A. The Terminating Access Provider (TAP) may charge the Originating Access Provider (OAP) upto Rs. 0.05 (five paisa only) per minute for A2P calls; Provided that there shall be no termination charge on: - (i) any A2P calls made by or on behalf of the Central Government or State Government; (ii) any A2P calls made by or on behalf of bodies established under the Constitution; (iii) any A2P calls made by or on the directions of the Authority; (iv) any A2P calls made by any agency authorized by the Authority from time to time; (v) any A2P calls made by			**1.Limited Effectiveness of Pricing as a Deterrent** • There is limited evidence to suggest that deterrent charges alone can significantly reduce UCC/spam. • In the A2P SMS segment, despite the existence of 5p IUC since inception, UCC concerns persisted until DLT-based/system-driven controls were implemented. • This indicates that pricing measures alone may not address the root cause of unsolicited communications. **2.Structural Advantage for Large Terminating Access Providers (TAPs)** •The proposed framework permits only TAPs to levy termination charges.

	using number resources assigned from 140xx, 1600xx or any other series designated by the Authority for commercial communications from time to time.			• Operators with a large subscriber base may benefit through higher terminating traffic volumes and on-net traffic advantages. • This may create an inherent advantage for large mobility operators. **3.Risk of Pricing Distortion** • Operators with a substantial on-net base may have greater flexibility to offer discounted enterprise communication pricing and absorb interconnect costs. • Similar practices are already visible in A2P SMS and toll-free service pricing. • This may result in uneven market dynamics and reduced customer choice. **4. Risk of Traffic Diversion Instead of UCC Reduction** • The proposed mechanism may shift traffic towards operators with stronger on-net advantages. • It may also encourage routing decisions based on cost arbitrage rather than service efficiency. • Such outcomes may not effectively address unsolicited communication practices. **5.Impact on Competitive Neutrality**

				• The framework may strengthen larger operators while increasing cost pressures on smaller and niche providers, particularly enterprise/wireline operators. • Over time, this may affect their sustainability and participation in the market. • It may also lead to market consolidation, contrary to the objective of a level playing field. **6.Suggested Way Forward** • If pricing is adopted as a deterrent, a balanced approach may be considered by: • Applying deterrent measures at originating and not at terminating access providers. • Introducing TRAI-led audit mechanisms and guardrails to monitor tariffs and prevent misuse. • Ensuring competitive neutrality across all categories of operators. **Conclusion:** A calibrated and equitable implementation of deterrent measures would better support the objective of curbing UCC while ensuring fairness, sustainability, and healthy competition across the

				telecom ecosystem.
	Schedule 1			
(59)	4	c) linking of the entity with a unique mobile number: Provided that the authority may, from time to time, prescribe any other manner of verification and authentication of the entities for the registration of senders and telemarketers by the access providers.		
(60)	2 h)	ensure that short code 127xxx, or any other code as prescribed by the Authority, shall be used by all Access Providers for sending consent seeking message related messages;		
(61)		(m) Primary Registration and Secondary validation of Content Templates for Service and Transactional Messages: (i) At the time of registration of SMS Content Templates, primary registration shall be undertaken by any one Access Provider, in accordance with the provisions of these regulations		**1.** It is submitted that the **volume of content templates across the ecosystem is significantly large**, and a blanket requirement for pre-validation by all Access Providers will not be technically feasible and may result in substantial operational and system-level challenges.

		and the Directions issued by the Authority from time to time. The Sender shall clearly indicate, at the stage of primary registration, the intended category of commercial communication, namely Promotional, Service, Transactional or Government, and shall complete all applicable formalities at that stage; (ii) Upon approval of a Content Template by the Access Provider undertaking primary registration, every other Access Provider shall, prior to acceptance of traffic, carry out secondary validation of the Content Template registered under Service and Transactional Message categories, by using the information available on DLT platform about such content template, for the limited purpose of verifying the correctness of its categorization under these regulations. No additional documentation or procedural formality shall be required to be completed by the Sender for the purpose of secondary validation		

		undertaken by other Access Providers: Provided that the Authority may, from time to time, prescribe the scope, manner and additional checks, if any, to be undertaken during such secondary validation, as well as the timelines for completion of secondary validation; (iii) Each Access Provider shall be independently responsible for ensuring compliance with these regulations and the directions of the Authority in respect of the categorisation of Content Templates accepted on its network, and also be liable for any breach thereof, irrespective of the categorization approved by the Access Provider that has carried out the primary registration of such Content Template.		

Additional inputs:

1. The term **Enterprise Registered Subscriber** for voice communications should be clearly defined in the Regulations. Pre-registration of subscriber numbers (CLI), along with the purpose of calls on the DLT platform, may be mandated to facilitate complaint resolution and reduce ambiguity through an additional layer of verification.

2. Any exceptions offered to a specific set of industry/sector/use case like Banks, Govt, Election campaigns by TRAI should be made formally made part of the Regulation so that may be defined as part of TSPs CoP for consistency to avoid any ambiguity.
3. The obligations prescribed under these Regulations may be more appropriately assigned to Registered Senders/Principal Entities (PEs) and Telemarketers (TMs), as they are directly responsible for the origination, content, and intent of commercial communications.
4. CNAP functionality for name tagging may be introduced for wireline enterprise operators also, to enhance caller identification and consumer awareness.
5. A standardized agreement, in line with the Regulations and supported by provisions for an additional security deposit, may be prescribed.
6. The responsibilities and obligations of VNOs should be clearly defined under the Regulations.
7. Clarity may be provided regarding AGR pass-through treatment of DCA charges between TAPs and OAPs.
8. A separate numbering series to be introduced for service and transactional calls for non-BFSI sectors before making regulation amendment effective
9. Clarity on election campaign related A2P calling and action process to be defined. For enterprises cost of connectivity is incurred by Telco therefore non declaring of A2P by the sender should not lead to impact Telcos in case regulation propose an action on sender.
10. There are cases where it is observed that standard scrubbing is not implemented at Preference level (1-8) , while few implement scrubbing logic at null or 0 preference. It leads to wrong closure of complaints for come telcos and penalty is levied on wrong closure. Wrongly routed complaints to be corrected.
11. Pre regulatory checks at TAP should be made mandatory to make UCC complaint handling more effective and genuine complaints only are actioned to save time and efforts. For example CDR not available, time window lapsed, reopening of complaints etc.
12. No process for change of address in case of secondary registration of TM . While new documents for change in address is taken but DLT address remains different as taken by the primary registrar.