STPL's 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.	~~(3) These shall come into force after ***thirty days*** from the date of their publication in the Official Gazette.~~ "These Regulations shall come into force on such date(s) as may be specified by the Authority. The Authority may notify phased timelines for implementation of various provisions of these Regulations in consultation with Telecom Service Providers and other stakeholders"	1. The provision prescribing a uniform implementation timeline of thirty (30) days from the date of notification may not be operationally feasible, considering the wide-ranging scope and complexity of the proposed amendments. 2. The draft amendments entail significant changes across regulatory, technical, and operational domains, which may require alignment with multiple stakeholders such as Principal Entities (PEs), Telemarketers (TMs), and technology providers. 3. In this regard, it is submitted that the timelines for implementation may be finalised in consultation with TSPs after issuance of the final regulations, 4. Further, it is submitted that a **phased implementation framework** would be more appropriate and effective, wherein the critical provisions may be prioritise for implementation.

(2)	**2. Definitions - In these regulations, unless the context otherwise requires**	after clause 2 (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 individual telecom subscriber, including using autodialling, robo-calls and/ or prerecorded/ artificial voice technologies."*	~~*"(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 individual telecom subscriber, including using autodialling, robo-calls and/ or prerecorded/ artificial voice technologies."*~~	1. It is submitted that there may not be a requirement to introduce a separate definition of "A2P Calls" within the TCCCP Regulations. The Regulations already define "Commercial Communication" under Clause 2(i), which adequately encompasses all forms of commercial interactions, including both Application-to-Person (A2P) and Person-to-Person (P2P) communications. 2. The proposed definition seeks to classify calls based on the mode of origination. However, in practical scenarios, it is challenging for TSPs to reliably and consistently determine whether a call has been initiated through an application or through human intervention. 3. With the increasing convergence of communication technologies, including the use of enterprise communication platforms, the distinction between A2P and P2P calls becomes blurred and difficult to enforce from a network and compliance standpoint.

				4. The inclusion of A2P as a distinct category may result in ambiguity in interpretation. Further, the usage of the term "A2P Calls" in subsequent provisions of the Regulations may not accurately capture the intended scope of commercial communications and may lead to inconsistencies in implementation across TSPs.
(3)		for clause 2(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."*		
(4)		in clause 2 (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 2 (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 previously terminated by either party;" ~~(iv) 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;~~		
(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 number resources allotted to 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."	(1) Every Access Provider shall ensure that any commercial communication using its network takes place only using registered headers or the resources allotted to 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 after Consultation and /discussion with TSPs"	1. It is submitted that the proposed proviso may have significant operational, technical, and compliance implications for TSPs. 2. Accordingly, it is essential that such classifications are formulated after consultation/ discussion with TSPs, to ensure feasibility of implementation, and alignment with existing architectures. 3.This approach would enable incorporation of practical insights from TSPs and facilitate smoother and timely implementation of this provision.
(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		4, Intimation regarding use of ~~A2P~~ Commercial calls – Every Sender shall declare to – the Originating Access Provider, in advance, about the use of ~~Application-to-Person (A2P)~~ Commercial calls. - 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	1. It is submitted that the term "A2P Calls" may be replaced with "Commercial Calls." As already highlighted above, "Commercial Communication" is defined under Clause 2(i) of the principal Regulations and encompasses all forms of commercial interactions, including both A2P and P2P communications. 2. This will avoid ambiguity and provide consistency across the regulatory

	shall take action against such sender as per the provisions of these regulations."		against such sender as per the provisions of these regulations."	framework. 3. Further the obligation to declare the nature and purpose of commercial communications should rest with the Sender/Principal Entity (PE), 4. Accordingly, it is suggested that the provision may clearly specify that the Sender shall provide prior declaration in respect of commercial calls to the concerned Access Provider, in accordance with prescribed formats and procedures 5. The current draft Amendment may be interpreted to place an implicit responsibility on TSPs to ensure compliance with such declarations. It is submitted that TSPs may not have visibility or control over the intent or classification of calls at the originating stage. 6. Thus, Imposing such obligations on TSPs may not be operationally feasible and may lead to undue compliance burden. 7. It is also submitted that the primary responsibility for ensuring compliance with declaration requirements should lie with Telemarketers (TMs) and

				Principal Entities (PEs), who are directly involved in the origination and dissemination of commercial communications. These entities are best placed to accurately classify communications and ensure adherence to regulatory requirements, including prior declaration and registration.
(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	(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	This clause is part of TRAI's Direction dated 27 February 2026 and is currently under deliberation with the Authority and TSPs and STPL shall align with the outcomes of the discussions. Further the	

	in accordance with Schedule IV, every access provider shall implement the following :-	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);	Authority is requested to kindly consider STPL's submission under letter no STPL/Reg/TRAI/2603/105 dated 28 March 2026.	
(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 of sending UCC (spam)"; Provided that the authority may prescribe the format and manner of sending such notification from time to time.		
(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 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;		
(17)		(d) upon identification of all the telecom resources allotted to such Sender, as referred in the preceding para, all the Access Providers including OAP, shall examine, within next one business day, whether any other CLI allotted to the same Sender has been flagged as "Suspected UCC CLI" by their respective AI/ML-based spam alert systems during the preceding ten days, and all such flagged CLIs mapped to the same sender shall be recorded and shared on DLT platform by all the Access Providers on the same day;		
(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 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 licence 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 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~~	The obligations under this clause shall be applicable to Registered Senders/Principal Entities and Telemarketers, as may be specified by the Authority. Access Providers shall facilitate implementation of such provisions in accordance with the Regulations, without being assigned primary responsibility for enforcement of compliance by senders."	1. It is submitted that obligations prescribed in these Regulations may be more appropriately assigned to **Registered Senders/Principal Entities (PEs)** and **Telemarketers (TMs)**, who are directly responsible for the origination, content, and intent of commercial communications. 2. Placing enforcement responsibilities on TSPs—particularly in matters requiring determination of compliance by senders—

		~~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;~~		may not be operationally feasible. Imposing such obligations could also lead to practical challenges in implementation, including increased compliance burden without commensurate control mechanisms. 3. For effective enforcement of the regulatory framework, it is essential that accountability is placed on entities that are directly involved in generating and transmitting commercial communications, i.e., Registered Senders/PEs and TMs.
(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.		
(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.		
(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 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	~~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 Appellate Authority shall resolve and reply to~~	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. 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 2.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 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.

		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."	~~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."~~	1. 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. 2. 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)	24) Distributed 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:	~~(i) to record three years history of complainant with details of all complaint(s) made by him, with date(s) and time(s), and status of resolution of complaints;~~		**1.** The draft provision mandates Access Providers (TSPs) to maintain a complainant-wise history for a period of three years, including details of complaints, appeals (if any), alleged violations, timestamps, status of resolution, as well as supporting documents relied upon for resolving such complaints. While the objective of
(29)		"(3) to record three years' history, complainant-wise, with details of all complaints including appeal, if any and alleged violations reported by the	"to record ~~three~~ two years' history, complainant-wise, with details of all complaints including appeal, if any and alleged violations reported by	

		complainants, with date and time, and status of resolution of complaints including the supporting documents used by the access providers for resolving the complaints;"	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;" The requirement to maintain supporting documents shall be limited to essential metadata or summary records necessary for audit and verification purposes.	enhancing traceability and accountability is appreciated, the scope of the requirement, particularly with respect to storage of supporting documents, presents significant operational challenges. 2. **Concerns regarding storage of the supporting documents:** The requirement to store "supporting documents" and artifacts associated with complaint resolution would result in the generation and retention of **substantial volumes of data**. It is submitted that existing platforms of DLT and CRM systems are not designed to store such large volumes of data over extended periods. Further, Compliance with this requirement would necessitate considerable augmentation of storage infrastructure, leading to increased cost, and system complexity. 3. **Consent registration Framework (CRF):** In this regard, it is submitted that the intended objectives of verification, traceability, and accountability may be more effectively achieved through the **implementation of the CRF.** This will reduce reliance on post-facto storage of extensive supporting artifacts, while ensuring verifiable and auditable
(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;		

				records of consent and communication flows. **4. Existing Data Retention Norms** It is further submitted that, as per licensing conditions, Call Detail Records (CDRs) and related information are required to be retained for a period of two (2) years. It is suggested that the retention period prescribed under this provision may also be aligned to **two (2) years**, instead of three (3) years.
(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 which the UCC complaint has been			
(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 direction, specify the content and method of making such communication to the complainant;		

	made.):-	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;		
(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 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		
(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 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.		
(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 sub-regulation (6);		
(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 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;		
(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 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;		
(46)		b iii) 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 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	For the purpose of audit of complaint handling process, the terminating and originating access	**1.** It is submitted that, in current operational practice, TSPs do not maintain or access CDRs in a manner that enables direct retrieval and sharing for individual

		the requested CDRs of the relevant period to the Authority.	providers shall provide ~~the requested CDRs of the relevant period to the Authority~~. relevant information, records, or system-based validation outputs pertaining to the reported communication, as may be required by the Authority.	complaint validation purposes. Complaint verification is typically carried out through system-based queries and validation tools, which confirm whether the reported communication (call/SMS) has occurred, along with limited associated parameters required for resolution. As such, the requirement to provide full CDRs for audit purposes may not align with existing system architecture and operational processes. **2.** The blanket requirement to provide CDRs for audit purposes may impose operational challenges, including the need for system modifications, Further, providing full CDRs may not be necessary for achieving the objective of auditing complaint handling processes, where limited and relevant data points would suffice. **3.** Thus, it is submitted that audit requirements may be aligned with existing operational practices, i.e. Validation of complaints may be undertaken through system-based query outputs; and only **relevant and limited information/metadata** necessary for audit purposes may be shared with the Authority, instead of full CDRs.

(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:	1 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 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.		
(49)		1 b) if the Access Provider has not fulfilled its obligations as envisaged in the regulations in respect of Header registration function and Content Templates registration function, it shall, without prejudice to any penalty which may be imposed under the terms and conditions of its licence or under any Act for the time being in force, be liable to pay, by way of financial disincentive, an amount of five thousand rupees per count of registration found not to be in accordance with these regulations.	~~1 b) if the Access Provider has not fulfilled its obligations as envisaged in the regulations in respect of Header registration function and Content Templates registration function, it shall, without prejudice to any penalty which may be imposed under the terms and conditions of its licence or under any Act for the time being in force, be liable to pay, by way of financial disincentive, an amount of five thousand rupees per count of registration found not to be in accordance with these regulations.~~	**1.** It is submitted that the Authority has already prescribed penal provisions in respect of incorrect categorisation of content templates, and cases where content templates are registered under an incorrect category by the OAP or other Access Providers. These provisions adequately address instances of non-compliance and ensure accountability within the ecosystem **2.** In this regard, we would like to submit that the introduction of an additional financial disincentive under Clause 27(1)(b), for similar instances relating to header and content template registration, is not required. Such overlapping provisions may result in disproportionate penal consequences and ambiguity in enforcement. **3.** It is submitted that regulatory measures, particularly those involving financial disincentives, should adhere to the principles of non-duplication, and clarity. **4.** Multiple prescribed penalties for similar

				violations may impose undue burden on TSPs without necessarily improving compliance outcomes. **5.** Thus, this Clause need to be deleted.
(50) (51)	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,	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 If the Authority finds that conclusion of the investigation conducted by the Access Provider is based on evidence but the sender or telemarketer satisfies the Authority that it has taken reasonable steps to prevent the recurrence of such contravention, the Authority may by order direct the Access Providers to restore the telecom resources of the sender or telemarketer, partially or fully; and delete the name and address of such sender or telemarketer from the blacklist,		It is submitted that the operationalization of such restoration requires careful consideration of certain technical and network-related constraints. **1. SIP & DID Connections** :It is submitted that restoration of resources such as **SIP connections and Direct Inward Dialling (DID) numbers** may not always be technically feasible once such resources have been deactivated, reconfigured, or reallocated within network systems. In many cases, these resources are dynamically managed and may not be capable of being restored in their original configuration, particularly after deactivation due to regulatory action. **2. Port-out Scenarios** In cases where the concerned sender or telemarketer has **ported out** telecom resources to another Access Provider, the OAP may not have the ability to restore such resources. This creates ambiguity in responsibility and feasibility, and may lead to implementation challenges.

		as the case may be, on payment of a restoration charge of five thousand rupees per resource to the Authority for restoration of all such telecom resources, subject to the condition that the total amount payable by the sender or telemarketer shall not exceed five lakh rupees: 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 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.		**3. Constraints due to Number Lifecycle** Telecom resources, including numbering resources, are subject to defined lifecycle management practices, including **recycling periods (e.g., 90-day cycles)**.Once a number/resource has entered the recycling pool or has been reassigned, restoration to the original entity may not be feasible due to operational and regulatory constraints, as well as risks of misrouting or misuse.
(52) (53)	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	(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		**1.** In this regard, it is respectfully submitted that such applications operate outside the direct control and network domain of TSPs. Accordingly, the **onus of ensuring compliance by such applications should not be placed on TSPs**, as they neither own nor control these platforms. The ecosystem of call management applications includes: a. Native handset-based dialers

	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 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~~.	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.		(controlled by device manufacturers/OS providers); and b. Third-party applications These entities fall outside the telecom regulatory domain of Access Providers, and therefore, compliance obligations, including reporting formats, data transmission, and accuracy of reporting, should be **directly assigned to such application providers**. 2. It is further submitted that provisions relating to call management applications may be addressed under a **separate and clearly defined regulatory framework or section**, given their distinct nature, stakeholders, and operational characteristics. Clubbing such obligations within TSP-centric provisions may lead to ambiguity in roles and responsibilities, and practical challenges in enforcement. 3. Also, The provision does not specify the legal basis or enforcement framework under which compliance by such applications (particularly third-party apps and handset manufacturers) would be ensured. In this regard, clarity is required on the applicable legal framework (including provisions under the Information Technology Act and related rules**)** under which action may

				be taken against non-compliant entities. Absent such clarity, enforcement of the provision may be difficult and may lead to regulatory uncertainty.
(54)		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/		

		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 using		This clause should be deleted.	The proposed insertion of Clause 35A, enabling Terminating Access Providers (TAPs) to levy a charge of up to ₹0.05 per minute on A2P calls, may not be appropriate and requires reconsideration. At the outset, the issue of Unsolicited Commercial Communications (UCC), including spam calls, is already comprehensively governed under the existing TCCCPR framework, which provides for robust, technology-driven controls such as DLT-based scrubbing, consent management, header and template verification, AI/ML-based detection systems, and strict penal provisions including suspension, disconnection, and blacklisting of telecom resources. In view of this, introduction of a pricing-based

	number resources assigned from 140xx, 1600xx or any other series designated by the Authority for commercial communications from time to time.			mechanism does not address any identified regulatory gap. It is further submitted that such charges are unlikely to act as an effective deterrent against non-compliant entities, who typically operate outside the regulated ecosystem and do not adhere to prescribed frameworks. On the contrary, the proposed provision may result in **additional cost burden on legitimate and compliant A2P communications**, which form a critical part of service delivery across sectors including banking, financial services, healthcare, and governance. Further, telecom charging principles have traditionally been based on the "work done" by the network. A2P calls do not impose any incremental cost on the network vis-à-vis other voice calls. Therefore, introduction of differential charges based on the nature of communication is not aligned with established regulatory and interconnection principles. It is also relevant to note that imposition of such charges may lead to **market distortions**, including migration of traffic to alternate platforms outside the regulatory

				framework, thereby potentially undermining the very objective of ensuring traceability and control over commercial communications. In view of the above, it is submitted that the proposed Clause 35A may not be introduced, and the Authority may instead continue to focus on strengthening existing compliance and enforcement mechanisms under the TCCCPR framework. Aside to above, we also request the Authority to kindly consider STPL's comments/ counter comments on similar issue as highlighted in the recent Consultation Paper on Review of existing TRAI Regulations on Interconnection matters dated 10 November 2025.
	Schedule 1			
	4	a) The registration process of Sender and the Telemarketers by Access Providers shall include- (a) physical verification of the entity;	The registration process of Sender and the Telemarketers by Access Providers shall include- ~~(a) physical verification of the entity;~~	**1.** It is submitted that existing Know Your Customer (KYC) norms prescribed under the licensing framework by the Department of Telecommunications (DoT) do not mandate physical verification and instead rely on **digital and document-based verification mechanisms**.

				2. The requirement for physical verification under the present Regulations would therefore be **inconsistent with the prevailing regulatory and licensing framework** and may lead to duplication of processes. **3.** With the availability of secure and scalable digital verification methods (including document verification, Aadhaar-based authentication, digital KYC, and other electronic processes), the objectives of authenticity and traceability can be effectively achieved **without requiring physical verification**. **4.** Such digital processes are also aligned with the Government's broader objective of promoting **ease of doing business and digital governance**. **5.** Thus, the requirement for physical verification is impractical, unsupported by the existing regulatory framework, lacks any scientific or factual analysis-based rationale, and unlikely to yield any tangible benefits, while imposing significant and unnecessary operational and cost burdens to the tune of thousands of crores on service providers.

(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.	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 after after consultation/ discussion with TSPs and other stakeholders	It is essential that manner of verification and authentication of the entities for the registration of senders and telemarketers by the access providers are formulated by TRAI after consultation/ discussion with TSPs, to ensure feasibility of implementation, and alignment with existing norms
(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 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,		**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 may result in substantial operational and system-level challenges. **2.** Such an approach may lead to delays, duplication of efforts, and increased processing load across networks, without proportionate incremental benefit. **3.** It is submitted that a more efficient and practical approach would be to undertake

		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 categorisation 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		**secondary validation at the stage when traffic is actually initiated using the concerned content template**. **4.** Such a traffic-triggered validation mechanism would ensure validation is carried out only for **active and relevant templates**; reduce unnecessary processing of dormant or unused templates; enable better utilisation of system resources; and facilitate more accurate validation based on actual usage context.

		Authority in respect of the categorisation of Content Templates accepted on its network, and also be liable for any breach thereof, irrespective of the categorisation approved by the Access Provider that has carried out the primary registration of such Content Template.		