COAI Response on TRAI Draft Telecom Commercial Communication Preference (Third Amendment) Regulations, 2026

COAI thanks the Authority for giving us an opportunity to offer comments on the important consultation on **Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026. Our submissions on key issues under discussion are in following paras.**

A. Leveraging AI/ML based spam flagging to control UCC-Industry's alternative proposal on Alternate Framework to Achieve TRAI's Objectives on UCC Control

1. COAI vide its letter DG/COAI/TECH/2026/3021 dated 27 March 2026 has submitted Industry's alternate proposal to leverage AI/ML-based spam detection systems deployed by TSPs. In this regard, it is respectfully requested that the Authority may consider and accept the proposed framework to enable its expeditious implementation in the interest of strengthening spam mitigation efforts.

B. Optimum approach to handle UCC

2. We are of the view that the Regulations i.e. Telecom Unsolicited Commercial Communications Regulations, 2007 dated 5th June 2007, followed by Telecom Commercial Communications Customer Preference Regulations, 2010 dated 1st December 2010 (with 16 amendments and several Directions) and the latest one Telecom Commercial Communications Customer Preference Regulations, 2018 dated 19th July 2018 followed by innumerable directions has not been effectively able to address the menace of UCC.

3. We are of the view that the indirect and penalty-based (through Financial Disincentive) approach adopted by the Authority on TSPs, who are only intermediaries and have no control over the content of the call/message, has not been successful.

4. **We submit that the optimum approach to handle this issue is to completely revamp the TCCCPR 2018 and make all individuals, Principal Entities (PEs) and all the Registered and Unregistered Telemarketers with Delivery Function/ Aggregator Function responsible for any violations**.

5. **The Telemarketer-Delivery (TM-D) should be brought under the licensing regime** with sufficient financial eligibility requirement to ensure that only serious players get involved and the Government and Authority have sufficient legal control over this entity to ensure compliance with TCCCPR-2018.

6. The responsibility of TSPs, being intermediary, should be limited to registering the preferences and consents of telecom subscribers, handling complaints, and communicating such complaints to the concerned TM-D. The TM-D should take action against the responsible Telemarketer- Aggregator (TM-As) and PEs. Any financial disincentive or penalty should be directly applicable to the licensed TM-D, who is

handing over the A2P traffic to the TSPs. In addition, the rules to be framed by the Government under the Telecommunication Act 2023 should have adequate provisions which empowers DoT to take deterrent actions directly against the individuals, companies, abettors, conspirators, including PEs, Aggregators and Telemarketers, who misuse the telecom resources for initiating UCC.

7. Further, it is recommended that **entire UCC regulatory framework may be reviewed holistically and aligned with the provisions under 'The Telecommunication Act 2023', so that we are able to find a best fit that will benefit all stakeholders i.e. consumers, telecom service providers(TSPs), PEs, Government, Exchequer and the other entities involved in this ecosystem**.

C. Alignment with the Telecommunication Act 2023

8. It is a well-established position that neither the TRAI Act 1997 nor the Indian Telegraph Act 1885 provide for a specific provision to empower the TRAI to act against unsolicited commercial communication. However, considering that UCC was an emergent issue that required to be addressed, the TRAI had issued the Regulations under Section 36 read with Section 11(1)(b)(v) of the TRAI Act. However, the Section 11 (1)(b)(v) of the TRAI Act is relating to QoS and states as follows:

"(v) lay-down the standards of quality of service to be provided by the service providers and ensure the quality of service and conduct the periodical survey of such service provided by the service providers so as to protect interest of the consumers of telecommunication service;"

9. Further, the Definition of Quality of service as per the QoS regulation i.e. 'Standards of Quality of Service of Basic Telephone Service (wireline) and Cellular Mobile Telephone Service Regulations, 2009' notified by TRAI is:

Regulation 2 (r) "Quality of Service" is the main indicator of the performance of a telecommunication network and of the degree to which such network conforms to the standards of such quality of service as specified in these regulations for specified parameters;

10. In similar vein, the Definition of Quality of service as per the Unified licence agreement is:

"77. QUALITY OF SERVICE: Quality of Service is evaluated on the basis of observable measure on the grade of service, Calls lost due to wrong processing, the bit error rate or the response time and also includes acceptable grade of number of faults per unit population of the subscriber served, the mean time to restore (MTTR), faults carried over beyond the MTTR and the satisfactory disposal thereof."

11. It is evident from the above that regulation of Quality of service issued by TRAI pertains only to regulation of the Quality of calls/ Data/ Messages. **The content of Calls and SMS is not under the purview of 'Quality of Service' Regulations. Therefore, the**

issues covered in TCCCPR 2018 have nothing to do with the Quality of service and should be addressed under different provisions.

12. With the enactment of 'The Telecommunication Act, 2023 wherein section 28 of the Act is specifically dedicated to measures for protection of users, the Authority must review and align the TCCCPR regulations with section 28 of 'The Telecommunication Act, 2023'.

13. Pertinently, with the enactment of the Telecommunication Act, 2023, the Parliament has empowered the Department of Telecommunication to directly take action against the users who are initiating unsolicited communication. Section 28 provides for measures for the protection of users. It empowers the Central Government to publish rules providing measures for protection of users in consonance with existing regulations of the TRAI (TCCCPR). The relevant section is reproduced below for ready reference:

28. (1) For the purposes of this section, "specified message" means any message, offering, advertising or promoting goods, services, interest in property, business opportunity, employment opportunity or investment opportunity, whether or not—
(a) the goods, services, interest, or opportunity are real; or
(b) it is lawful to acquire such goods, services, property, interest or take up the opportunity.
(2) The Central Government may by rules provide for measures for protection of users, in consonance with any regulations notified by the Telecom Regulatory Authority of India from time to time, including measures such as…. (Emphasis added)

14. Clearly, this provision empowers DoT to take any measure for the protection of users. It is inclusive in nature, allowing broad measures to stop the menace of such calls at the root, i.e., at the users' level. The provision allows the Department to take direct action against users initiating unsolicited communication for the misuse of an allocated telecommunication resource.

15. Further, Section 33 of the Telecommunication Act, 2023 provides that under the Adjudication Mechanism provided by the legislation, the Adjudicating Officer (AO) can conduct an inquiry and pass an order imposing civil penalty upto the amount specified in the Third Schedule which will be payable by the person committing such contravention. Sl. No. 3 of the Third Schedule provides for a penalty for the contravention of Section 28 – this permits the AO to act against users initiating unsolicited communication as well as others such as the abettors and conspirators (such as Principal Entities, Telemarketers, etc. as defined by the TCCCPR). These have been extracted below.

33. (1) The Adjudicating Officer shall, upon receipt of a complaint in such form, manner and accompanied by such fees as may be prescribed, relating to contravention of this Act as specified in the Third Schedule, or suo motu, conduct an inquiry under the provisions of this Chapter, pass an order in

writing specifying the civil penalty up to an amount as specified in the Third Schedule, payable by the person committing such contravention.
(2) The provisions of the Third Schedule shall apply to the abetment of, or attempt to commit, or conspiracy to commit such contravention, as they apply to such contravention. **(Emphasis added)**

16. In light of the above, **the Department can frame detailed rules to directly take action against users that initiate unsolicited communication on receiving a complaint from the receivers of unsolicited communication without making TSPs disconnect connections indirectly**. Additionally, it can take action not only against these users but also against those abetting, attempting to commit, or conspiring to commit a violation of Section 28, which has been extracted above.

17. This implies that in case of unsolicited communication regarding banking services or any other service, not only the user making the call, but also those conspiring (agencies, banks, individuals – referred to as Principal Entities under the TCCCPR) can be acted against. Additionally, the Department can also act against telemarketers and other aggregators of calls / messages who are reselling services. Therefore, **the Authority may kindly initiate consultation to recommend to the DOT, the terms and condition of the rules to be framed for measures for protection of users** and any fine tuning of the TCCCPR-2018 in its current and unproductive framework should be put on back burner till formulation of said Rules.

D. Critical need to bring Reseller of services i.e. Telemarketer under licensing framework.

18. The A2P traffic originates from about 2,80,000 Principal Entities (PE), it is then aggregated by about 16000 Aggregator Telemarketer (TM-A) and these TM-As deliver this traffic to about 15 Delivery Telemarketers (TM-D). **These 15 TM-D are connected to every TSPs and handovers the A2P traffic to TSPs. Thus, the only entity directly interacting with TSPs for all practical purposes is the TM-D. Consequently, the TSPs are completely dependent on TM-Ds to identify TM-As and PEs and find it difficult to identify, leave alone punish the source in case of transmission of UCC/ Fraud Messages.**

19. In the earlier UCC Regulations i.e. TCCCPR-2010, the Telemarketers were registered with TRAI and with DoT in 2007. However, TRAI through TCCCPR-2018, asked TSPs to register these telemarketers. But due to the limitations of the market structure in SMS business, this approach has proved to be ineffective. **Thus, it is important to take the major step of bringing the TM-D under licensing framework in order to effectively control the UCC menace as well as fraudulent messages.**

20. It is pertinent to note here that by its very function, **TM-D is clearly a reseller of services and should be either licensed like VNO or should be authorized by DoT under the upcoming authorization regime under Indian Telecommunication Act 2023**. Considering the significant role of TM-D in handling the UCC, there should be sufficiently high financial eligibility requirements to become an authorised TM-D, to ensure adequate deterrence against wilful violations.

21. This will be a far-reaching step and would impact the UCC landscape considerably as when the TM-Ds is an authorized entity duly registered by DoT, it will be easier for the DoT to control their practices and thereby fraud. Further the DoT LSA units can be leveraged for vigilance and inspection of the TM-D and PEs, in case of any violations.

22. DoT is already having very effective vigilance set-up at DoT LSA level. Further, DoT has also taken initiative of Chakshu Portal, to curb the fraudulent calls. The coordination with LEAs will also be easier, if it is done under the aegis of DoT.

E. TSPs are intermediaries and cannot be made accountable/ penalised for UCC.

23. Vide Regulation 27 of the TCCCPR-2018, the Authority has prescribed Financial Disincentives (FD) on Access Providers for failure to curb the UCC from registered Senders/ RTMs. Further, vide the current consultation process, the Authority proposes to expand the scope of FDs under regulation 27 to headers and templates. The Authority also proposes to impose FDs on access providers for failure to curb the UCC from unregistered senders/ UTMs by amending the regulation 28 of TCCCPR. However, these FDs are not based on legal grounds and are in violation of the law of the land. We submit that before any review of the existing provisions of the Regulations issued by the Authority in 2018, the Authority must take into the account the relevant provisions of **'Information Technology Act, 2000'.**

24. **As per the Section 79 of the Information Technology Act, TSPs are merely intermediaries (and therefore, exempted from liability), hence, TSPs cannot be held accountable or penalised for unsolicited communication being done using their network.** The relevant Section 79 of the Information Technology Act, 2000 is reproduced below for ready reference.

79. Exemption from liability of intermediary in certain cases.–(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if–
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
(b) the intermediary does not–
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf…. (*Emphasis added*)

25. As can be inferred from the above, TSPs are mere carriers, and their function is limited to providing access to the communication system. They do not initiate the transmission, select the receiver or modify the information contained in the transmission. Therefore, they qualify as exempted intermediaries under Section 79.

26. Keeping in mind the larger interest of users, TSPs have implemented mechanisms such as Blockchain DLT, spam filtering, scrubbing, etc. in an attempt to reduce the occurrence of such calling. All these measures are non-intrusive in nature, i.e., without storing or tampering with the information contained in the transmission.

27. **However, these mere acts of facilitating a Regulation made by the sector regulator does not imply that the TSPs are responsible for compliance with the Regulation by other stakeholders in the ecosystem. Consequently, TSPs cannot be penalized for UCC being initiated by other stakeholders.**

28. Furthermore, it is submitted that under the Unified License Security conditions, the bonafide use of telecom services is the responsibility of the subscriber and TSPs are required to make the same clear to the subscribers, which is being done. Thus, the TSPs cannot be held responsible for non-bonafide use in manner of UCC by the subscribers. We are extracting and reproducing the relevant clause for ready reference.

39.17 (i) The Licensee shall ensure adequate verification of each and every customer before enrolling him as a subscriber; instructions issued by the Licensor in this regard from time to time shall be scrupulously followed. The Licensee shall make it clear to the subscriber that the subscriber will be responsible for proper and bonafide use of the service.

F. TRAI does not have powers under the TRAI Act to penalise the TSPs.

29. The preamble of TRAI Act provides for the Authority to protect the interests of service providers and consumers of the telecom sector, to promote and ensure orderly growth of the telecom sector. However, it is respectfully submitted that the dispensation under the TCCCPR, 2018 appears to have limited provisions addressing the interests of service providers. In contrast, TSPs have been entrusted with extensive responsibilities, including the registration of entities, their headers and content templates, as well as the registration of telemarketers, under the framework of co-regulation.

30. This fact has also been acknowledged by the Authority itself in its Consultation Paper on UCC dated 20.11.2006. In para 3.38 of the said Consultation Paper, TRAI noted, inter alia, that *"**The Authority does not have adequate and effective power in enforcing and penalizing violators. It has formally proposed to the DoT for a comprehensive amendment in the TRAI Act to strengthen powers of the Authority in terms of penalty as provided in most of the countries**."*

31. Thus, even while initiating steps to curb unsolicited commercial communications, TRAI acknowledged that it did not have the power under its parent statute, the TRAI Act, to

impose penalties for violations of the Regulations. The amendments to the TRAI Act called for in the Consultation Paper have not been carried out till date.

32. Thereafter, TRAI issued Telecom Unsolicited Commercial Communication Regulation, 2007 (4 of 2007) dated 05.06.2007. In para 28 of the Explanatory Memorandum to 2007 Regulation, TRAI had clarified and reiterated that it did not have any power either to impose penalty or to adjudicate the complaints and that therefore, TRAI had decided to follow the route of levying higher tariffs on those telemarketers who violate the Do Not Call List. The relevant portions of para 28 of the Explanatory Memorandum to said Regulation are reproduced hereunder:

28. "… Some views have been expressed that a tariff recovered by the service provider should be passed on to the affected subscriber. However, it is clarified that TRAI has neither any power to impose penalty nor power to adjudicate the complaints……" (Emphasis supplied)

G. Licensees have no power to penalise their consumers:

33. The Regulations have provided limited provisions and rights to TSPs to control the UCC menace, however, the same are neither practical nor implementable. Regulation 22 of the TCCCPR-2018 is reproduced below for ready reference:

*"22**. Prescription of fee/ charges by Access Providers: Access Providers may prescribe fee from participating entities for sending commercial communications for registration and to carry out activities provided for in these regulations and may also prescribe security deposits. Access providers may impose financial disincentive on participating entities in case violation of regulations can be attributed to failure of functions assigned to such entities."***

34. As per the above provision, TSPs are permitted to impose FDs on its own customers i.e. PEs/ TMs, however, this provision overlooks the fact that the TSPs do not have any collective powers under their license agreement to impose/ recover penalty/ FDs from their consumers. **Further, the language of the said provision of the regulation makes it an optional activity and does not provide an express mandate backed by the law, leaving it open to multiple interpretations and implementations.**

35. Due to the extremely competitive commercial communication market with multiple players like PSUs, private operators without spectrum but access service authorization, and TSPs, the task of recovering FDs from PEs, is not possible for TSPs. As any coercive action can lead to churn and customer poaching by the competition, who are having access service authorization without any frequency spectrum.

36. Clearly, the only effective way to bring discipline in UCC/ SPAM/ Fraud menace is a centralized and uniform implementation and that is possible only **if DoT directly imposes the penalty on TM-D/ PEs, who are actually responsible for the UCC.**

H. No adjudicatory powers with TRAI

37. There are various provisions of TCCCPR discussed in the consultation paper, providing filing of an Appeal before the Authority e.g. Regulation 25 (6); Regulation 33(2). It is important to note that TRAI does not have adjudicatory power under the TRAI Act. Further, as per The Telecommunication Act, 2023, any Appeal can be filed before the DoT appointed adjudicating officer/ Designated Appeals Committee (Please refer Chapter VIII of The Telecommunication Act, 2023). Therefore, these provisions are ultra-vires.

I. No action on the Parallel spam market on OTT

38. Further, it is respectfully submitted that despite various representations made by the industry, no action has been taken by the Government and Regulator on parallel promotional and service messaging channels like IP messages by handset vendors and promotional communications disseminated through OTT applications.

39. It is reiterated that these alternate and substitutable channels are undermining the effectiveness of the DLT-based UCC framework, as they enable similar services to be offered to the same set of customers without being subject to comparable regulatory checks and requirements.

40. By not regulating these channels, a legal and controlled SMS channel is being cannibalized by illegal services running without any regulatory oversight. As a double whammy, the TSPs that are investing millions for controlling UCC are being served FD notices, that too for a fraction of incidents compared to those occurring on these unregulated channels unabated. It is pertinent to mention here that ever increasing stringency by Authority on SMS channel is accelerating the shift of traffic from regulated SMS channel to unregulated channels like IP messages and OTTs**.**

41. **It is also not out of place to mention here that not just spam, these unregulated channels are the chief abettors of fraud by carrying fraud URLs/APKs/CTAs in their transmissions which can be clicked open immediately as these services are already operating on broadband.**

42. Furthermore, it is submitted there is no explanation given regarding the continued hosting of screen-mirroring software and APKs by search engines and application platforms, and the facilitation of their widespread download, which have reportedly been associated with financial fraud incidents globally.

43. It is respectfully requested that the Authority may consider formulation of a **technology-neutral, proportionate, and risk-based regulatory framework** applicable across all communication platforms offering person-to-person (P2P) voice, messaging, and video services in India, including but not limited to VoLTE, VoNR, RCS, and App based OTT platforms.

44. It is further submitted that neither the Telecommunications Act, 2023 nor the TRAI Act, 1999 envisages differential treatment between comparable communication services

based solely on the network/platform architecture. Accordingly, selective regulation of TSPs without corresponding obligations on functionally similar platforms-based service providers may lead to a non-level playing field and dilute overall consumer protection objectives.

45. The regulatory framework may, *inter alia*, **ensure uniform accountability across all P2P communication service providers.** It should mandate baseline fraud prevention and consumer protection safeguards. Such safeguards should enable coordinated intelligence sharing and real-time response mechanisms across platforms. Further, **the framework must minimize regulatory arbitrage and prevent the migration of fraudulent activities between platforms. This, in turn, will strengthen India's overall digital trust and safety architecture.**

46. It is submitted that such a framework would not impede innovation; rather, it would ensure that innovation progresses in tandem with consumer protection. Fragmented or platform-specific approaches, however well-intentioned, risk perpetuating misuse by enabling regulatory gaps.

47. The Authority may also consider providing further guidance on the measures in place to address the optimization and dissemination of potentially malicious web links and applications, particularly with respect to due diligence requirements. These aspects indicate regulatory gaps which, it is submitted, may benefit from a more holistic and consistent approach to ensure effective mitigation of such risks across the ecosystem.

48. The Authority is, therefore, requested to adopt a **holistic and technology-neutral approach to address spam and digital communication-based fraud, and extending proportionate regulatory safeguards across all relevant platforms.**

COAI 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.	~~(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 prioritised 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."*		Our members might comment on this Regulation individually.
(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."*		It is also pertinent to mention that TSPs don't have any mechanism of verifying the Consents. If the process followed under the CRF Pilot is to be followed, the consents have to be recorded on the DLT platform basis a declaration from PE that the said consents are lawful and valid. There is no check possible at TSP end and hence, such compliance should be mandated at PE level and compliance is also assessed directly through PE.
(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		We are okay with proposed change

		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."	"(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."	We would like to submit that the term "live testing" should be removed from the definition of Regulatory Sandbox as testing is done in secured environment.

(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;~~	(e) 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 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; **(iii) for business related enquiries made by a subscriber**"	1. A legitimate enquiry from a business forms the basis of a relationship and leads to genuine calls. For instance, a query to yellow pages type online aggregator is supposed to result in callbacks by the businesses serving the customer requirements. However, the period of such calls can be restricted. To deal with such legitimate enquiries, we are suggesting addition in the definition of Service Message or Service Call in Regulation 2(bh). 2. At the same time, it may be noted that such definitions are subjective and the best party to ensure compliance is Principal Entity and hence, the related compliance should be applied directly on them.
(7)		in clause (bh), (i) its Customer or		1. As mentioned in the justifications

		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:	For clarity in the suggested additions, reproducing the complete definition of Service Message or Service Call: "Service Message or Service Call" means a message sent or voice call made by a sender to- (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 Consent from the Recipient and such messages or voice calls are not promotional in nature:	given in response to 2(bb) above, a legitimate enquiry from a business leads to genuine calls. Inclusion of this, in the definition of service call will address this issue and the period of such calls can also be restricted to 7 days. 2. Explicit consent is recorded in the CRF and remains valid until the subscriber revokes it. In the definition, use of words "explicit consent" and limiting it to a period of seven days creates ambiguity and confusion. Therefore, it is suggested that the term 'explicit' be deleted.

			(iii) a recipient to respond/ fulfil business related enquiries made by him/her" Provided that such Consent shall be for seven days or as directed by the Authority from time to time: Provided further that a transactional Message or transactional Voice Call containing information pertaining to service shall be treated as a Service Message or Service Voice Call;	
(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;~~		We strongly recommend that App-based communication service providers should also be included for the purpose of application of regulatory norms on commercial communication and for protection of consumers from spam.
(9)		clause (bo), "Telecom resources" means any ~~telegraph~~ telecommunication equipment and/or telecommunication		We are okay with proposed change

		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;~~		We are okay with proposed change
(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 proposed in the present consultation itself, to ensure that the complaint handling process remains seamless and is not impeded due to the absence of such prior classification. **3.** Further, we would like to submit that COAI vide its letter dated DG/COAI/TECH/2025/3111 dated 11 November 2025 has submitted Enterprise and Individual UTM Complaint Handling Mechanism with

				the timelines and the thresholds for taking actions on the complaints. We request TRAI to kindly consider the submitted process favorably and accordingly issue appropriate Directions for the implementation of the same.
(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."			Our members might comment on this Regulation individually.
(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		We are okay with proposed change

		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);	Clause to be removed and replaced by a new one basis the proposal shared by COAI vide its letter DG/COAI/TECH/2026/ 3021 dated 27 March 2026 with TRAI.	1. AI/ML-based detection systems deployed by TSPs inherently generate outputs across **varying levels of confidence**. Not all such outputs represent definitive spam activity. 2. Treating all flagged instances as actionable may lead to a large number of **false positives**, resulting in unintended hardship to legitimate subscribers, including genuine enterprises and individuals engaged in lawful communication. 3. Considering that mobile phones have become a critical identity and lifeline for consumers—enabling banking, payments, e-commerce, and e-governance—any wrongful disconnection or restriction of services can cause significant unintended hardship to legitimate users due to false positive flagging. Therefore, any regulatory intervention must be carefully
(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.		designed to ensure that such hardship is avoided, and legitimate consumers are adequately protected. 4. Further, a large-scale action against the false positive cases may cause panic with customers Not only will this disrupt their experience of using telecom services but will also distress them in turn to start calling the customer care and saturate the TSP's capability to address the customer's queries. 5. Accordingly, **regulatory enforcement should be restricted to high-confidence cases**, where there is strong and corroborated evidence of spam behaviour, ensuring that actions are accurate, proportionate, and defensible. 6. To enable consistency and avoid fragmented implementation, TSPs shall agree on the criteria for classification of **high confidence suspected spam**
(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 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~~	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 and directly assigned as well as enforced by the TRAI on the **Registered Senders/Principal Entities (PEs)** and **Telemarketers (TMs)**, who are directly responsible for the origination, content, and intent of commercial communications. **2.** Delegating enforcement responsibilities on TSPs—particularly in matters requiring determination of compliance by senders—may not be operationally feasible and is also structurally not aligned as TSPs are also one of the actors in the

		~~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;~~		commercial ecosystem. 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. **4.** Further, we request that the definition of misuse may kindly be provided in the Regulation itself.
(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	~~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~~	**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

		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.”	~~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.”~~	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. **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. **5.** 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. **6.** Besides, most of the complaints in UCC are closed through system response in automated way, as such, registration of appeals through a separate process, will not lead to any

				different outcome.
(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 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
(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 ~~three~~ one year 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;" The requirement to maintain supporting documents shall be limited to essential metadata or summary records necessary for audit and verification purposes.	

(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;		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 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 one (1) year. It is suggested that the retention period prescribed under this provision may also be aligned to **one (1) year**, 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 made.):-			
(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; Provided further that every complaint reported by the customers after seven days but before the lapse of fifteen days of receipt of the unsolicited commercial communication by the customers, shall be recorded by the		Our members might comment on this Regulation individually.

		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		We are okay with proposed change
(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		We are okay with proposed change

		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		We are okay with proposed change

		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:		We are okay with proposed change
(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;		We are okay with proposed change
(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		We are okay with proposed change

		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;		1. It is not possible to keep so much variable in the process based on an entity, both technically as well as operationally.

		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.		2. Further, such comprehensive and granular information for classifying the senders in different categories, is not part of any onboarding/KYC guidelines and hence, is not available with TSPs. 3. Such extensive and micro regulatory actions would cause more and more operational hassles as well as will be prone to non-compliance. 4. The Authority is requested to explicitly notify these entities and the first list may be notified with the Regulations itself. The differentiated criteria for action against Enterprise and Govt entities may be defined here and not kept subjective, else we will keep struggling with action against such accounts. Industry has already shared a differentiated action plan for Enterprise customers, same may be used here. 5. In absence of the same, unless an entity is explicitly notified by Authority, the TSP will not be able to treat it any differently.
(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		We are okay with proposed change

		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);~~		We are okay with proposed change
(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		We are okay with proposed change

		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		1. Such comprehensive and granular information for classifying the senders in different categories is not part of any onboarding/KYC guidelines and hence, is not available with TSPs. 2. Such extensive and micro regulatory actions would cause more and more operational hassles as well as will be prone to non-compliance. 3. The Authority is requested to explicitly notify these entities and the first list may be notified with the Regulations itself. The differentiated criteria for action against Enterprise and Govt entities may be defined here and not kept subjective, else we will keep struggling with action against such accounts. Industry has

		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;		already shared a differentiated action plan for Enterprise customers, same may be used here. 4. In absence of the same, unless an entity is explicitly notified by Authority, the TSP will not be able to treat it any differently.
(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		We are okay with proposed change

		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		We are okay with proposed change

		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		**1.** Such comprehensive and granular information for classifying the senders in different categories, is not part of any onboarding/KYC guidelines and hence, is not available with TSPs. **2.** Such extensive and micro regulatory actions would cause more and more operational hassles as well as will be prone to non-compliance. **3.** The Authority is requested to explicitly notify these entities and the first list may be notified with the Regulations itself. The differentiated criteria for action against Enterprise and Govt entities may be defined here and not kept subjective, else we will keep struggling with action against such accounts. Industry has already shared a differentiated action plan for Enterprise customers, same may be

		differentiated sets of enforcement measures applicable to such categories of senders for violations of these regulations.		used here. **4.** In absence of the same, unless an entity is explicitly notified by Authority, the TSP will not be able to treat it any differently.
(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.		We are okay with proposed change
(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.	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~~. relevant information, records, or system-based validation outputs pertaining to the reported communication, as may be required by the Authority.	**1.** Under the license and present legal provisions, the CDRs are maintained in utmost secured way and is provided, on demand, only to the security agencies designated by the DoT. As such, we request that no provisions related to CDRs should be brought under TRAI Regulations. **2.** Also, 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 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. **3.** 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. **4.** 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	1 a) without prejudice to any penalty which may be imposed under its licence or under any Act for the time	~~1 a) without prejudice to any penalty which may be imposed under its licence or under any Act~~	**1.** It is respectfully submitted that the imposition of Financial Disincentives on TSPs may merit reconsideration. The Action should be taken by TRAI

	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:	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	~~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,~~	directly against the offending senders and suitable provisions are incorporated in this Regulation. **2.** Without prejudice to the above, if the Content Templates are registered under wrong category by another Access Provider and the traffic has been sent by the OAP under that category, then the Access Provider who has registered in the wrong category is only responsible. The OAP has no control over such messages as the template has been approved by another TSP and is available as approved template on DLT. **3.** Hence, prospectively financial disincentives be primarily anchored at the point of enterprise onboarding and header/template registration, where the ability to prevent misuse is most effective. Registrar TSPs, being directly responsible for validation and compliance at this stage, are best placed to ensure adherence to regulatory requirements. **4.** The Authority may also consider adding a provision about timelines beyond which complaints/alleged instances of violation may not be eligible for examination.

		as well as the access provider that has registered such Content Templates under 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 license 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 Regulation need to be deleted.
	28)	1 d) if the Access Provider is found to have misreported the count of UCC for UTMs, it shall, without prejudice to any penalty which may be imposed under the terms and conditions of its licensor any other provisions under these regulations, be liable to pay, by way of financial disincentive, an amount of two lakhs rupees: Provided that if the Access Provider is found to have misreported the count of UCC for UTMs consecutively in two or more subsequent months, the Access Provider shall be liable to pay, by way of financial disincentives, an amount of five lakhs rupees for the second consecutive misreporting and ten lakhs rupees for each consecutive misreporting occurring		**1.** It is respectfully submitted that the provision does not specify timelines within which the Authority may seek supporting data, records, or artifacts from Access Providers for verification of reported UCC counts. **2.** In the absence of clearly defined timelines, there may be uncertainty for TSPs in terms of data availability, retention, and readiness for audit or verification, particularly given existing data retention timelines prescribed under licensing conditions. **3.** Accordingly, it is essential that specific timelines be prescribed within which such information may be sought by the Authority. **4.** As per existing licensing conditions, relevant telecom data (including CDR-related information) is typically

		thereafter: Provided further that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider has been given a reasonable opportunity of representing.		retained for a defined period (e.g., one year). **5.** Therefore, any requirement for submission of supporting artifacts or validation data must be aligned with such retention periods,
(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 f 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		We are okay with proposed change

		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, 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.		

(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 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~~			**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 (controlled by device manufacturers/OS providers); and b. Third-party applications 2. 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**. Besides, there should be clear audit provisions to ensure that the process implemented by these entities are non-repudiable and also to ensure check on the veracity of the information basis which action is expected from TSPs.
(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.		

	~~enforcement measures, against non-compliant Call Management Applications in coordination with relevant authorities, if required~~.			
(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;		We are okay with proposed change
(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		We are okay with proposed change
(57)		35 ii) any message transmitted by or on behalf ~~the directions~~ of bodies established under the Constitution;		We are okay with proposed change
(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 number resources assigned from 140xx, 1600xx or any other series			Our members might comment on this Regulation individually.

	designated by the Authority for commercial communications from time to time.			
	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.** Further, It is a known fact that Aadhaar based eKYC process is the most secured, preferred & encrypted consent-based authentication mechanism for issuing SIMs to the subscribers. Hence, eKYC not only constitutes over 95% of the new SIM activations, but the process is also widely used for SIM exchanges and re

				verification of subscribers. It is important to note that the eKYC process ensures capturing of live photo of the subscriber & matching it with photo received from UIDAI, capturing of geo-coordinates of the place where KYC is being done and can only be performed through a Registered Point of Sale (PoS) which is onboarded through eKYC, as per instructions contained in DoT circular dated 31.08.2023. Hence there is no merit in performing physical verification of subscribers. **4.** 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**. **5.** Such digital processes are also aligned with the Government's broader objective of promoting **ease of doing business and digital governance**. **6.** 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, 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 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.		
	4)	8) Voice Calling Function with Telecom Resource Connectivity (VCF)a) deliver voice calls to OAP, in a secure and safe manner, during specified time slots and types of days of delivery in accordance to the preferences of the customer(s);	~~deliver voice calls to OAP, in a secure and safe manner, during specified time slots and types of days of delivery in accordance to the preferences of the customer(s);~~	Entity with VCF does not have access to preference data only OAP can do the needful scrubbing based on preference

	5)	2) Consent Registrar (CR) to b) establish Customer Consent Verification Facility (CCVF) for the purpose of facilitating: customers to verify, modify, renew or revoke their consent in respect of commercial communications, and	~~establish Customer Consent Verification Facility (CCVF) for the purpose of facilitating: customers to verify, modify, renew or revoke their consent in respect of commercial communications, and~~	As per the current DCA process TSPs do not verify the Consent. TSP only record the consent, the responsibility of the verification of the consent is of PEs.
	5)	Telemarketer for voice calling function with Telecom Resource Connectivity for voice calls to Access Provider (TM-VCF) to		TM do not have access to preference and consent registry and hence cannot perform this activity.

****