TO BE PUBLISHED IN THE GAZETTE OF INDIA, EXTRAORDINARY, PART III, SECTION 4

TELECOM REGULATORY AUTHORITY OF INDIA
NOTIFICATION
New Delhi, the 18th September, 2026

TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCE (THIRD AMENDMENT) REGULATIONS, 2026

(05 of 2026)

No. RG-25/(25)/2023-QoS: - In exercise of the powers conferred upon it by section 36, read with sub-clause (v) of clause (b) and clause (c) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act 1997 (24 of 1997), the Telecom Regulatory Authority of India hereby makes the following regulations further to amend the Telecom Commercial Communications Customer Preference Regulations, 2018 (6 of 2018), namely:-

1. Short title, extent and commencement. —
   (1) These regulations may be called the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 (05 of 2026).
   (2) These regulations shall apply throughout the territory of India.
   (3) These regulations shall come into force after thirty days from the date of their publication in the Official Gazette except-
      (a) regulation 4, regulation 6, regulation 8(a) and regulation 18, which shall come into force after sixty days; and
      (b) the amendments listed in Annexure, which shall come into force after ninety days,
   from the date of their publication in the Official Gazette, respectively.

2. In regulation 2 of the Telecom Commercial Communications Customer Preference Regulations, 2018 (6 of 2018) (hereinafter referred to as the "principal regulations"), --

(a) after clause (e) the following clause shall be inserted, namely:-
"(ea) "Application-to-Person call or A2P 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 pre-recorded/ artificial voice technologies;";

(b) for clause (k), the following clause and explanation thereto shall be substituted, namely:-
"(k) ***"Consent"*** *means any voluntary permission, either explicit or inferred, given by the customer to Sender to receive Commercial Communication related to specific purpose, product or service.*
Explanation 1.— For the purposes of these regulations, the expression 'consent' is limited to the voluntary permission given by the customer to the Sender for the establishment of communication channel between the Sender and the customer for Commercial Communications, as agreed to between them.
Explanation 2.— For the purposes of these regulations, the expression 'revocation of consent' is limited to the withdrawal of the voluntary permission referred to in Explanation 1, by the customer.
Explanation 3.— Nothing contained in these regulations shall exempt the Sender from its obligations, or liability under the Digital Personal Data Protection Act, 2023;";

(c) for clause (y), the following clause shall be substituted, namely: -
"(y) "Explicit Consent" means consent which has either been 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 from time to time;";

18/09/2026
हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(d) in clause (ah), the first proviso, "Provided that such consent shall not extend beyond duration / discharge of the contract between the Sender and the Recipient:" shall be deleted;

(e) in clause (ai), for the words "clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885)", the words "*clause (g) of section 2 of the Telecommunications Act, 2023 (44 of 2023)*" shall be substituted;

(f) for clause (ba), the following clause shall be substituted, namely:-

"(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 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;";

(g) 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 an inquiry for goods or products or services, submitted by the Recipient to Sender within seven days immediately preceding the date of the receiving of communication, which relationship has not been previously terminated by either party:

Provided that such an inquiry shall be made in writing or through digital means, and shall be maintained in a verifiable form by the Sender;

(iii) 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;";

(h) for clause (bh), the following clause shall be substituted, namely:-

"(bh) ***"Service message or Service Call"*** *means a message sent or voice call made by a Sender to –*

(i) *its Customer to provide information pertaining to a product or service procured by such customer, its warranty or service, 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, OTPs for authentication, such as app login, password reset, two-factor authentication etc., and such messages or voice calls are not promotional in nature and do not require Explicit Consent; or*

(ii) *a Recipient to facilitate 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:*

Provided that such Explicit Consent shall be valid for a period of seven days or until revoked by the customer, whichever is earlier, and it may be renewed at the instance of the customer for an additional period of seven days at a time:

Provided further that the Authority may specify the validity period of such Explicit Consent from time to time:

Provided also that a transactional Message or transactional Voice Call containing information pertaining to service shall be treated as a Service Message or Service Voice Call;";

(i) in clause (bn), for the words "a telecom service provided by an Access Provider" the words *"any service for telecommunication"* shall be substituted;

(j) after clause (bm) the following clauses shall be inserted, namely:-

"(bma) "Spam" means Unsolicited commercial communication as defined in clause (bw) of this regulation;

(bmb) "Spammer" means a Sender or Telemarketer engaged in sending Unsolicited commercial communication;";

(k) in clause (bo), for the word "telegraph", the words *"telecommunication equipment and/or telecommunication identifier, as defined under the Telecommunications Act, 2023 (44 of 2023),"* shall be substituted;

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(l) in clause (bt), the words "apps login" appearing after the words "non-bank-entities like e-commerce" shall be deleted.

3. In regulation 3 of the principal regulations, in sub-regulation (1), the following proviso shall be inserted, namely: -

"Provided that the Authority may classify the Senders for this purpose and may specify different criteria for different classes of Senders."

4. For regulation 4 of the principal regulations, the following regulation shall be substituted, namely:-

"4. Intimation regarding use of A2P calls. —

Every Sender shall declare to the Originating Access Provider (OAP), in advance, about the use of Application-to-Person (A2P) calls, along with the details such as Calling Line Identification (CLI) ranges to be used for making A2P calls, or any other details as specified by the Authority from time to time, and such declaration shall be recorded on the DLT platform by the OAP along with the levels/series/ numbering resources assigned to such Sender:

Provided that any such call made by a Sender without prior declaration to the OAP, shall be treated as Unsolicited commercial communication, and the OAP shall take action against such Sender as per the provisions of these regulations."

5. In regulation 11 of the principal regulations, in sub-regulation (4), the words "put under usage cap or his telecom resources may be" appearing after the words "failing which the telecom resources used or assigned to him may be" shall be deleted.

6. In regulation 13 of the principal regulations, the following proviso shall be inserted, namely:-

"Provided that in case of a Virtual Network Operator (VNO), the concerned Network Service Operator (NSO) shall provide the necessary digital interface having real time functionality with DLT platform and any other system to enable the VNO to perform its obligations under these regulations:

Provided further that the Authority may specify the mechanism to provide such digital interface to VNOs by the NSOs from time to time."

7. After regulation 21 of the principal regulations, the following regulation shall be inserted, namely:-

"21A. (1) Every Terminating Access Provider (TAP), shall, through the AI/ML-based UCC_Detect system established by it in accordance with Schedule IV, identify from among the Calling Line Identifications (CLIs) flagged as suspected of sending Unsolicited commercial communication (UCC), and flag the Calling Line Identification (CLI) of the Sender, having high probability of being engaged in sending UCC, as "Suspected high probability UCC CLI" based upon the behavioural parameters, and immediately upon such identification and in any case, within two hours of such identification, share such CLIs with the concerned Originating Access Providers (OAPs) through the Distributed Ledger Technology (DLT) platform:

Provided that the Authority may specify the parameters for identifying the Calling Line Identification (CLI) of the Sender as "Suspected high probability UCC CLI" from time to time:

Provided further that based on the technical considerations, the Authority may specify any other mechanism for sharing the information from time to time:

Provided also that no CLI from 140xx series, 1600xx series, 1601xx series, or any other numbering series specially designated by the Authority for Commercial Communications and notified for the purpose of this proviso, shall be flagged as "Suspected UCC/spam" for the Recipients:

Provided also that the Access Provider shall provide a mechanism to the Senders whose CLIs have been flagged as "Suspected UCC/spam" to represent against such flagging, with justification, and shall unflag the CLIs if justification is found in order:

Provided further that the Authority may also specify the mechanism to unflag the CLIs by the Access Providers from time to time.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(2) *Every OAP shall, upon receipt of the intimation regarding "Suspected high probability UCC CLI" flagging from the TAP, immediately issue a notification through SMS or email or both, to the Sender associated with such CLI, informing that based on communication behaviour, the CLI has been identified as suspected of sending UCC.*

(3) *The OAP shall, within one business day of the receipt of these CLIs 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.*

(4) *Upon identification of all the telecom resources allotted to such Sender, as provided in sub-regulation (3) of this regulation, all Access Providers including OAP, shall examine, within the next business day, whether any other CLI allotted to the same Sender has been identified as "Suspected high probability UCC CLI" by their respective AI/ML-based spam alert systems during the preceding ten days, and all such identified CLIs mapped to the same Sender shall be recorded and shared on DLT platform by all the Access Providers on the same day.*

(5) *Upon receipt of the data of all the "Suspected high probability UCC CLIs" associated with such Sender across the network, 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 identified as "Suspected high probability UCC CLI" within a period of last ten days, and if it is found that five or more CLIs of the Sender have been so identified within the last ten days, all the concerned OAPs shall take action against the Sender as provided hereunder:*

(a) 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-

(a) where the KYC re-verification is unsuccessful, the OAP shall take necessary action in accordance with the extant KYC guidelines;

(b) where the KYC re-verification is successful, such instance shall nevertheless be treated as the first instance of violation, and any subsequent violation shall be considered as repeated violation under these regulations;

(b) for the second such instance, OAP shall, within the next five business days, carry out the physical KYC verification of the Sender and check that the telecom resources allotted by OAP are not being misused by the Sender for sending UCC and-

(i) 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, the 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;

(ii) where the KYC details of the Sender available with OAP match with the details obtained on physical verification, such instance shall nevertheless be treated as the second instance of violation, and any subsequent violation shall be considered as repeated violation under these regulations;

(c) for any such subsequent instance, the OAP shall, within the next five business days, check that the telecom resources allotted by it are not being misused by the Sender for sending UCC and 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."

8. In regulation 22 of the principal regulations, in sub-regulation (1), --

(a) for clause (a), the following clause shall be substituted, namely:-

"(a) in case of misuse of Headers or Content Templates,

(i) immediately upon noticing the misuse, but not beyond six hours of noticing such misuse, while acting as OAP, suspend such misused Header or Content Template across all Access Providers, as the case may

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

be; inform about such suspension of the Header or Content template to the Registrar Access Provider, and the OAP shall, within forty eight hours of receiving such report of misuse, issue a notice to the Sender in whose name such Header or Content Template is registered, and such suspension shall remain in force until the conditions specified under sub-clause (ii) are fully complied with by the Sender;

(ii) require the Sender to undertake all the following remedial actions:

(A) *reset, within three business days of receipt of notice from the Originating Access Provider, 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;*

(B) *file a formal complaint with the appropriate law enforcement agency under the applicable laws, within three business days of receipt of notice from the OAP, 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 within two business days of such filing:

Provided that, if it is found by the Sender or determined by the OAP that any Telemarketer has misused or the 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 and, without prejudice to any action that law enforcement agencies may take against such Telemarketer, the OAP shall bar all the outgoing services of such Telemarketer immediately, and issue a notice, within twenty four hours of such finding, to the Telemarketer to reply to the notice, with justification, within three business days and on receipt of reply from the Telemarketer or the expiry of notice period of three business days, whichever is earlier, if the OAP finally concludes that the misuse has been done by the Telemarketer or if the Telemarketer is an accomplice, all the telecom resources of such Telemarketer shall be disconnected across all the Access Providers for a period of one year and the Telemarketer shall be blacklisted during this period:

Provided further that, if it is conclusively determined that Sender is not at fault, all such headers, content templates and other resources suspended in compliance of sub- clause (i) of clause (a) of this sub-regulation shall be restored within two business days of such determination;

(C) *Where it is found by the Sender or determined by the OAP that misuse occurred due to leakage, cloning, or compromise of credentials, the Registrar Access Provider shall, within next five business days, mandatorily de-register all Headers and Content Templates of such Sender, including those reported as misused, to prevent any further misuse of leaked credentials, and intimate Sender within twenty four hours to get them re-registered and the Registrar Access Provider shall issue new header and content template ids during such re-registration.*

Provided that, where the Registrar Access Provider is satisfied that immediate bulk de-registration may materially disrupt essential Commercial Communications or cause significant inconvenience to the consumers, it may undertake such de-registration in a phased manner, subject to the condition that the entire de-registration process is completed within further five business days or such extended period as may be permitted by the Authority;

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(D) *Conduct within ten business days of receipt of notice from the OAP, a comprehensive review of all its registered Headers, Content Templates, Consent Templates; and 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;*

(iii) ensure that, where the Sender fails to fully comply with the obligations under sub-clause (ii) of clause (a) of this sub-regulation within the stipulated timeframe, or provides 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, specify any other procedures, safeguards, timelines, and conditions to safeguard the security of the Commercial Communications.

Explanation: For the purpose of this regulation, "misuse" means the unauthorized use of any Header or Content Template by any person or entity other than the Sender in whose name such Header or Content Template is registered, or any use by any person or entity resulting from compromise, theft, leakage, cloning, unauthorized access to credentials or systems, impersonation, etc.";

(b) in clause (i), the following proviso shall be inserted, namely:-
"Provided that the Authority may, for the purpose of preventing the misuse of telecom resources for sending UCC by the Sender or the Telemarketer, specify the essential conditions of the agreement between the Access Provider and the Sender or the Telemarketer, and that such conditions shall mandatorily form part of such agreement.".

9. In regulation 23 of the principal regulations, --

(a) in sub-regulation (1), after clause (b), the following clause shall be inserted, namely:-

"(c) (i) to prefer an appeal to the Appellate Authority, as provided in the Telecom Consumers Complaint Redressal Regulations, 2012 (1 of 2012), within a period of fifteen days from the date of receipt of information about the resolution of the complaint, or, if no intimation of redressal of the complaint is received by the complainant within a period of fifteen days from the date of registering complaint, then within next fifteen days from the date of lapse of such period.

(ii) The complainant shall be able to prefer such appeal through any of the modes specified for lodging a UCC complaint or report under the Telecom Commercial Communications Customer Preference Regulations, 2018, besides the modes provided for preferring appeal under Telecom Consumers Complaint Redressal Regulation, 2012.

(iii) The Appellate Authority shall resolve and reply to such appeal in the manner and within the period as provided in the Telecom Consumers Complaint Redressal Regulations, 2012 (1 of 2012).

(iv) The Access Providers shall establish the necessary mechanism for communicating the appeal received by the TAP to the concerned Appellate Authority at OAP within one business day, including the appeals received by the TAP through email, mobile application, website/portal, complaint centre, or post or in person.

(b) in proviso (a) to sub-regulation (5), for the words *"mobile number"*, wherever appearing, the word *"telephone number"* shall be substituted.

10. In regulation 24 of the principal regulations, --

(a) in sub-regulation (2), for the words "complaint or report regarding violation" the words *"complaint, including appeal, if any, or report regarding violation"* shall be substituted;

(b) for sub-regulation (3), the following sub-regulation shall be substituted, namely:-

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

"(3) to record two 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;";

(c) for sub-regulation (4), the following sub-regulation shall be substituted namely:-

"(4) to record two years' history of the Senders against whom complaints, including appeal, if any, have been made or reported, along with details of all complaints including appeal, if any, with date and time, and status of resolution of complaints;";

11. For regulation 25 of the principal regulations, the following regulation shall be substituted, namely:-

"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 detected as suspected of sending UCC with high probability, by the AI/ML based UCC detect systems across all the Access Providers; and take remedial action against Senders as provided hereunder:-

(1) Terminating Access Provider shall record the complaint and report on DL-Complaints in non- repudiable and immutable manner and shall notify, in real time, the details of the complaint to the concerned Originating Access Provider (OAP) except when it is not possible to do so as stipulated in sub-regulation (2).

(2) In instances where there is non-availability of complete telephone number of the Sender or Header in the complaint registered, TAP shall communicate to the Customer about the closure of his complaint, with reason, and educate the Customer about the correct manner of registering a complaint.

(3) 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 every complaint reported by the customers including those reported after seven days of the receipt of the Unsolicited commercial communication by the customers, shall be recorded by the Terminating Access Provider as well as the Originating Access Providers.

(4) In case the complaint is related to Registered Telemarketer or registered Sender, OAP shall-

(a) notify the receipt of the complaint to the Sender immediately with such details which helps the Sender to start the investigation immediately;

(b) examine communication detail records, within two business days from the date of receipt of complaint 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;

(c) in case of non-occurrence of complained communications under sub-regulation (4)(b), communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner as specified in the Codes of Practice:

(d) in case of occurrence of SMS-related complained communications under sub-regulation (4)(b), further examine, within 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-

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(i) *if all regulatory pre-checks were carried out and delivery of Commercial Communication to the Recipient was in conformity of the provisions of the regulations and Codes of Practice, communicate to TAP to inform complainant about the closure of complaint along with reasons as provided for in the Codes of Practice;*

(ii) *in case non-compliance with the regulations is found, take action against the defaulting entity as provided for in these regulations-supplemented with Codes of Practice, within three business days from the date of receipt of complaint by the OAP, and communicate to TAP to inform the complainant about the action taken against the complaint:*

Provided 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 during the last ninety days, the OAP shall suspend the services of the Sender, for one month or till the 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), examine, within 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 –*

(i) *in case, all regulatory pre-checks were carried out and delivery of Commercial Communication to the Recipient was in confirmation to the provisions in the regulations and Code(s) of Practice, communicate to TAP to inform complainant about the closure of complaint along with reasons as provided for in the Code(s) of Practice;*

(ii) *in case of non-compliance with the regulations, take action against the defaulting entity as provided for in these regulations and Codes of Practice, within three business days from the date of receipt of complaint by the OAP, and communicate to TAP to inform the complainant about the action taken against the complaint;*

(iii) *take appropriate remedial action, as provided for in the regulations, supplemented with the Code of Practice(s), to control Unsolicited commercial communications from such Senders so as to ensure compliance with these Regulations;*

(f) *in case of occurrence of complained communications under sub-regulation (4)(b) related to promotional Voice Calls made using the number resource(s) allotted from series assigned for transactional and service calls, the action shall be taken by the Access Provider as directed by the Authority from time to time.*

(5) *in case, the complaint is related to an Unregistered Telemarketer, OAP shall-*

(a) *intimate the receipt of the complaint to the Sender immediately;*

(b) *examine Communication Detail Records (CDRs), within two business days from the date of receipt of complaint by OAP, to check the occurrence of complained communication between the complainant and the reported telephone number from which Unsolicited commercial communication was received;*

(c) *in case of non- occurrence of complained communications under sub-regulation (5)(b), communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner as specified in the Codes of Practice;*

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(d) *in case of occurrence of complained communications under sub-regulation (5)(b), examine within a maximum time of further one business day, whether there are similar complaints or reports against the same Sender, and-*

(i) *if it is found that there are three or more complaints against the Sender from unique Recipients during the last ten days across all Access Providers, and also any CLI allotted to the Sender has been identified or maintained as "Suspected high probability 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 across all Access Providers, 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);*

(ii) *in case, it is found that number of complaints against the Sender are from less than five unique Recipients during last ten days across all Access Providers, and none of the CLIs of the Sender has been flagged or maintained as "Suspected high probability UCC CLI" by the AI system of the Access Providers during these last ten days across all Access Providers, the OAP shall communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner specified in the Codes of Practice.*

(6) *In case of occurrence of complained communications under sub-regulation (5)(d)(i) above, OAP shall, immediately issue a notice to the Sender to give opportunity to represent its case within five business days; thereafter, within five business days from the date of receipt of representation from the Sender, or in case, no reply is received from the Sender, then within five business days from the date of expiry of the period given to Sender for representing the case, whichever is earlier, investigate and record the reasons of its findings and in case the conclusion of OAP is that the Sender or its Telemarketer was engaged in sending the Unsolicited commercial communications, OAP shall take action against such Sender as under-*

(a) *for the first instance of violation, 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;*

(b) *for subsequent instances of violations, -*

(i) *all telecom resources including PRI/SIP trunks, SIMs etc. of the Sender shall be disconnected by all the Access Providers for one year, irrespective of whether those telecom resources were actually used or not in making such communications;*

(ii) *OAP shall put the Sender under the blacklist category during the period of one year as above and no new telecom resources shall be provided by any Access Provider to such Sender during this period;*

(iii) *all the devices used for making UCC shall also be blocked across all the Access Providers for a period of one year:*

Provided that one telephone number with outgoing services barred may be allowed to be retained by such Sender during this period, and notified emergency outgoing services should be allowed despite such outgoing services being barred on the permitted telephone number.

(7) *In case action is taken against a Sender under sub-regulation (4) or sub-regulation (6) of this regulation-*

(a) *the Sender can represent to the OAP against such action, and the OAP shall decide the representation within a maximum period of seven business days and shall record its findings.*

(b) *OAP shall file the details of all the representations decided by it to the Authority for regulatory review as per the format and periodicity specified by the Authority, from time to time.*

(c) *If the Sender is not satisfied with the decision of the OAP on its representation, the Sender may*

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

make a representation to the Authority against such decision of OAP, as provided under regulation 29.

Explanation: For the purpose of this regulation, Sender 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."

12. After regulation 25 of the principal regulations, the following regulation shall be inserted, namely:-

"25A. (1) The Authority may, from time to time, for the purpose of regulatory enforcement under these regulations, 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, 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) The Authority may, from time to time, for the purpose of ensuring effectiveness or consistency of the implementation of these regulations, may specify various operational measures as required under various provisions of these regulations;

(3) The Authority may, from time to time, publish in such form and manner as it considers appropriate, the details of the entities who have violated the provisions of the regulations."

13. In regulation 26 of the principal regulations, --

(a) after sub-regulation (2), the following sub-regulation shall be inserted, namely:-
"(2A) Every Access Provider shall maintain record of every alleged violation of the regulations, reported by its customers and shall also record reports of such alleged violations of the regulations received from the other Terminating Access Providers.";

(b) after sub-regulation 4, the following sub-regulation shall be inserted, namely:-
"(4A) For the purpose of audit of complaint handling process, the Terminating Access Providers and Originating Access Providers shall provide to the Authority such information, including CDRs of the relevant period, as the Authority may call for."

14. In regulation 27 of the principal regulations, --

(a) for the existing heading, the heading *"Consequences of failure to take action against registered Senders or RTMs for sending Unsolicited commercial communications"* shall be substituted;

(b) in sub-regulation (1), --

(i) for the words "to curb Unsolicited Commercial Communications from registered Senders or RTMs," appearing after the words "If an Access Provider fails" and before the words "the Authority may" , the words *"to take action against registered Senders or RTMs for sending Unsolicited commercial communications in accordance with the provisions of the regulations"* shall be substituted;

(ii) *in clause (a), for the existing proviso, the following provisos shall be substituted, namely: -*

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

"Provided that where UCC has originated due to failure of the OAP to carry out scrubbing in accordance with the preference and consent of the customer, OAP shall be liable to pay, by way of financial disincentive, an amount of one thousand rupees per count of such valid complaints:

Provided further 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 25 of these regulations, the financial disincentive as above shall be imposed on the Access Provider that has registered such Headers and Content Templates, instead of OAP."

15. For regulation 29 of the principal regulations, the following regulation shall be substituted, namely:-

*"**29. Representation by Senders or Telemarketers against the action taken by Access Providers.**— The Authority may, on receipt of a representation from the Sender or Telemarketer, within sixty days of action taken against it by the Access Provider under regulation 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,-*

(a) 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, subject to the feasibility, 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;

(b) if the Authority finds that conclusion of the investigation conducted by the Access Provider is based on evidence, but the Sender or Telemarketer satisfies the Authority that it has taken reasonable steps to prevent the recurrence of such contravention, the Authority may by order direct the Access Providers to restore the telecom resources of the Sender or Telemarketer, partially or fully, subject to the feasibility; 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 rupees five thousand 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 rupees five lakh:

Provided that in the case of PRI or SIP trunks, each DID number shall be treated as a separate telecom resource:

Provided further 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 under clause (b) of this sub-regulation shall not be less than half of the restoration charges calculated to restore all the telecom resources of the Sender or Telemarketer:

Provided also that the amount payable under clause (b) of this sub-regulation may be reduced or waived off by the Authority where it finds merit in the response furnished by the Sender or Telemarketer:

Provided that the Authority may, for reasons to be recorded in writing, consider the representation received from the Sender or Telemarketer after sixty days of action taken against it by the Access Provider under regulation 25:

Provided further that Authority may specify from time-to-time Standard Operating Procedures or issue directions or instructions detailing exact steps to be taken to decide such cases."

16. For regulation 34A of the principal regulations, the following regulation shall be substituted, namely:-

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

"34A. Prohibition on blocking of designated number series by Call Management Applications or similar services. —

(1) *No call management application or similar services that offers users a mechanism to report any UCC/ spam shall tag, block or filter incoming calls originating from any number series designated by the Authority or the Central Government for commercial and government communications, or treat such calls in any manner that is different from that applicable to genuine communication, or restrict or facilitate blanket tagging of such calls as spam or otherwise, conveying a similar meaning;*

Provided that consumers shall have the freedom to filter or block any calls on their own devices, at their personal discretion for their own purpose, but such individual actions shall not affect the settings, preferences or experience of any other Recipient or customer as far as incoming calls from any number series designated for Commercial Communications or government communications are concerned.

(2) *No call management app including phone diallers and third-party apps, shall offer the user of the app a mechanism to report any Unsolicited commercial communication under any name such as spam, junk, etc., which implies UCC, unless the call management application sends such report, to the DLT platform maintained by the Access Providers.*

(3) *In case, any call management application or similar service is found to be non-compliant with sub-regulations (1) and (2) of this regulation, the Authority may initiate action under the applicable laws for non-compliance. Provided that no order for initiating action under sub-regulation (3) shall be made by the Authority, unless the concerned entity has been given a reasonable opportunity to represent."*

17. In regulation 35 of the principal regulations,

(a) in the proviso in item (i) and (ii), for the words, *"by or on the directions of"*, the words, *"by or on behalf of"* shall be substituted.

(b) the following proviso shall be inserted before the existing proviso, namely:-
"Provided that such charge shall not be more than the lowest tariff offered by the Terminating Access Provider to the Senders or the Telemarketers for whom it acts as the Originating Access Provider."

18. After regulation 35 of the principal regulations, the following regulation shall be inserted, namely:-

"35A. The Terminating Access Provider (TAP) may charge the Originating Access Provider (OAP) upto Rs. 0.05 (five paisa only) per minute (on per minute pulse basis), for A2P calls:
Provided that such charge shall not be more than the lowest tariff offered by the Terminating Access Provider to the Senders or the Telemarketers for whom it acts as the Originating Access Provider:
Provided further that there shall be no such charge on -

(i) *any A2P calls made using number resources assigned from 140xx, 1600xx, 1601xx or any other series designated by the Authority for Commercial Communications from time to time unless notified to the contrary by the Authority;*
(ii) *any A2P calls made by or on the directions of the Authority;*
(iii) *any A2P calls made by any agency authorized by the Authority from time to time."*

19. In Schedule-I of the principal regulations, --

(a) in item 1, after proviso to sub-item (4), the following proviso shall be inserted, namely:

"Provided further that the Authority may, from time to time, specify any other manner of verification and authentication of the entities for the registration of Senders and Telemarketers by the Access Providers.";

(b) in item 4, sub-item (2), in entry (h), --

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(i) for the words "any other code as prescribed by the Authority", the words *"any other code or SMS headers as specified by the Authority"* shall be substituted;

(ii) for the words "seeking message", the words *"related messages"* shall be substituted.

20. In Schedule-II of the principal regulations, --

(a) in item 1, --

(i) for the existing heading, the heading *"Registration or change of preference of Categories of content for Commercial Communications:-" shall be substituted;*

(ii) for sub-item (1), the following sub-item shall be substituted, namely;

(1) *Customer can opt-out of any or all of the following Commercial Communications categories of content:*

Commercial Communications Category to be blocked or opted out	**IVRS: Call to 1909 and press at prompt to block**	**SMS: Send SMS to 1909 following text**	**USSD: Dia l USSD String**
Opting out of all Promotional Commercial Communications (CC)			
All Promotional CC Categories (to be blocked)	**50**	BLOCK PROMO	*1909*50#
Opting Out of specific categories of promotional CC			
Banking/Insurance/Financial products/ credit cards,	1	BLOCK 1	*1909*1#
Real Estate,	2	BLOCK 2	*1909*2#
Education,	3	BLOCK 3	*1909*3#
Health,	4	BLOCK 4	*1909*4#
Consumer goods and automobiles,	5	BLOCK 5	*1909*5#
Communication/Broadcasting/ Entertainment/IT,	6	BLOCK 6	*1909*6#
Tourism and Leisure,	7	BLOCK 7	*1909*7#
Food and Beverages,	8	BLOCK 8	*1909*8#

Note-1: In case of communication with customer executive of Customer Care Centre of Access Provider, customer may communicate his/ her preferences to be registered;

Note-2: Confirmation and final status along with options exercised to be communicated to the customer;

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

Note-3: BLOCK PROMO option shall block only promotional types of Commercial Communications for all categories of content, mode, time band and day types but shall not block transaction and service type of Commercial Communications and Government Communications;

Note-4: At the time of commencement of the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026, all preferences registered under FULLY BLOCK category shall be migrated to BLOCK PROMO category within fifteen days from the date of such commencement:

Provided that the Authority may, from time to time, add or remove number of categories, or sub-categories for content.";

(iii) for sub-item (2), the following sub-item shall be substituted, namely;

(2) Customer can opt-in for any or all of the following Commercial Communications categories of content:

UCC Category to be unblocked or opted in	IVRS: Call to 1909 and press at prompt to unblock	SMS to 1909 following text	USSD send
All Promotional Categories (to be unblocked)	90	UNBLOCK ALL	*#1909*90#
Opting in for specific categories			
Banking/Insurance/Financial products/ credit cards,	91	UNBLOCK 91	*#1909*91#
Real Estate,	92	UNBLOCK 92	*#1909*92#
Education,	93	UNBLOCK 93	*#1909*93#
Health,	94	UNBLOCK 94	*#1909*94#
Consumer goods and automobiles,	95	UNBLOCK 95	*#1909*95#
Communication/Broadcasting/ Entertainment/IT,	96	UNBLOCK 96	*#1909*96#
Tourism and Leisure,	97	UNBLOCK 97	*#1909*97#
Food and Beverages;	98	UNBLOCK 98	*#1909*98#

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

Note-1: In case of communication with customer executive of Customer Care Centre of Access Provider, customer may communicate his/ her preferences to be registered;

Note-2: Confirmation and final status, along with options exercised to be communicated to customer;

Note-3: UNBLOCK ALL option shall unblock all Promotional categories of content, mode, time band and day types with default options;

Note-4: UNBLOCK 51 shall stand deleted with effect from the sixteenth day from the date of commencement of the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026:

Provided that the Authority may, from time to time, add or remove number of categories, or subcategories for content;"

(b) in item 2, --

(i) for the existing heading, the heading "*Registration of preference or change of preference of Mode for Commercial Communications:-" shall be substituted;*

(ii) in sub-item (1),

(A) in Note 1, for the word "Center", the word "*Centre*" shall be substituted;

(B) in Note 3, for the words "except transactional type commercial communications", the words *"except transactional type and service type of Commercial Communications"* shall be substituted;

(iii) in sub-item (2), in Note 1, for the word "Center", the word "*Centre*" shall be substituted;

(c) in item 3, --

(i) in sub-item (1),

(A) in Note 2, for the word "Center", the word *"Centre"* shall be substituted;

(B) for Note 4, the following Note shall be substituted, namely:-

"Note-4: BLOCK 20 option shall block all categories of modes while saving current status of customer for categories of content, time band and day types. However, transactional type and service type of Commercial Communications shall not be blocked during any time band:"

(ii) in sub-item (2), in Note 1, for the word "Center", the word "*Centre*" shall be substituted;

(d) in item 4, --

(i) in sub-item (1),

(A) in Note 2, for the word "Center", the word "*Centre*" shall be substituted;

(B) for Note 4, the following Note shall be substituted, namely:-

"Note-4: BLOCK 30 option shall block all categories of types of days while saving the status of customer for categories of time band and day types. However, transactional type and service type of Commercial Communications shall not be blocked during any day type:"

(ii) in sub-item (2), in Note 1, for the word "Center", the word "*Centre*" shall be substituted;

(e) in item 6, in sub-item (2), for entry (b), the following entry shall be substituted, namely:-

"(b) Location Routing Number (LRN), as assigned by DoT to the Access Provider, of current serving network of the customer, and in case customer is being ported-in during Mobile Number Portability, the update in LRN of the new serving network to be done by the recipient Access Provider within twenty four hours of such porting into the new serving network through MNP process, in the manner as specified by Authority from time to time;"

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

21. In Schedule-IV of the principal regulations, in item 1, for sub-item (4), the following sub-item shall be substituted, namely:-

"(4) Access Providers shall, through SMS or email, intimate the Senders detected above that they have been identified as suspected UCC Senders with high probability of being engaged in sending UCC and that they must refrain from sending UCC, failing which action may be taken against them under the provisions of the regulations."

18/09/2026

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

(Harinder Kumar)
Secretary

Note 1: The principal regulations were published in the Gazette of India, Extraordinary, Part III, Section 4 vide notification No. 311-04/2017-QoS dated 19th July 2018 and amended vide:

(i) Notification No.- 311-04/2017- QoS dated 21st December, 2018 (10 of 2018).

(ii) Notification No.- RG-25/(25)/2023-QoS dated 12th February, 2025 (1 of 2025)

Note 2: The Explanatory Note explains the objects and reasons of these regulations.

Disclaimer: In case of any discrepancy between English version and Hindi version of these regulations, the English version shall prevail.

ANNEXURE

Specific amendments to come into force after ninety days from the date of publication in the Official Gazette

1. Regulation 9 (a) inserting 'Regulation 23(1)(c) of the Principal Regulations'
2. Regulation 11 amending 'main clause of Regulation 25 of the Principal Regulations' regarding "Corroboration of complaints data with the data of Senders detected as suspected of sending UCC with high probability".
3. Regulation 11 inserting 'Proviso to Regulation 25(4)(d)(ii) of the Principal Regulations'.

(Harinder Kumar)
Secretary

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

EXPLANATORY MEMORANDUM

1. **Effective date for the regulations to come into effect:**

   A. **Stakeholders' comments**

   a) In response, many stakeholders submitted for phased timelines for implementation of various provisions of these Regulations in consultation with Telecom Service Providers and other stakeholders.

   b) One stakeholder submitted that it should be at least 6 months in a phased manner from the date of their publication in the Official Gazette with due consideration of the suggested changes in the draft.

   B. **Analysis and conclusion:**

   i. Consultation on proposed amendments has already been conducted. The timelines have been mandated keeping in view the quantum of work for implementation of various regulations. It is also noted that some of the provisions of this amendment are already implemented or being implemented through the Directions issued earlier. Based on these considerations, the Authority has decided that the regulations shall come into force after *thirty days* from the date of their publication in the Official Gazette except for *regulations on Intimation regarding use of A2P calls including declaration of CLI ranges on DLT, Terminating charges for A2P calls, Digital interface with DLT to VNOs, and misuse of headers/ content templates,* which shall come into force after *sixty days,* and regulations *on appeal mechanism through DLT, corroboration of complaints with data of AI flagged suspected high probability UCC Senders, and suspension of services of the Sender for wrong categorisation of the content templates,* which shall come into force after *ninety days* from the date of their publication in the Official Gazette, respectively.

2. **'Consent': Amendment to Regulation 2(k)**

   A. **Stakeholders' comments**

   a) One of the stakeholders has suggested that there is need to clarify that the 'consent' under TCCCPR 2018 is not the same as the 'consent' under the DPDP Act, and that the use of the same term "consent" in TCCCPR is leading to confusion, ambiguity and unintended interpretations regarding the rights and obligations of customers, Senders and TSPs. The stakeholder commented that the intent of consent framework under TCCCPR was to enable consumer to seek support from their respective TSP for not receiving commercial communication traffic from a Sender, who claims it to be sent based on a permission received from consumer. While this permission is just for commercial communication, the consent under DPDP Act 2023 could be much wider and govern the broader aspects of personal data processing. The 'consent' under DPDP Act carries legal implications concerning collection, processing, storage, and use of personal data.

   b) It was also stated that 'revocation of consent' under TCCCPR, 2018, does not mean that the original 'consent' acquired under the framework of DPDP Act gets revoked. On the basis of revocation under the regulatory framework, the Sender would not be able to use voice/SMS for sending commercial communication to such customer. However, the Sender is free to process the consent under DPDP Act for servicing the consumer or sending communications through other means such as App-based communication services, emails etc. Therefore, 'revocation of consent' under TCCCPR 2018 is only stopping commercial communications through SMS/voice'.

   c) The stakeholder submitted that the Digital Consent Acquisition Pilot undertaken by TSPs with 11 Banks under the guidance and direction of TRAI, put forth clear expectation from Banks as well as TSPs that the Authority should address the confusion on consent under DPDP Act and consent under TCCCPR 2018.

   d) It was further suggested that to avoid such a confusion and to clearly distinguish the objective of the TCCCPR framework from the consent requirements under the DPDP Act, it is imperative that the term "consent" under TCCCPR is replaced with a more suitable expression such as "permission", or any other term that specifically reflects a customer's authorization to receive promotional communications and is also easy to understand by the consumer. Similarly, it was suggested to replace the term 'revocation' with a term

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

'suspension'. Such a distinction would provide greater regulatory clarity and facilitate easier understanding and implementation of the respective frameworks by all stakeholders.

e) It was suggested that in view of the above, the relevant clauses of TCCCP Regulation 2018 may be suitably modified.

B. Analysis and conclusion:

i. The Authority observes that while the "Explanation" to the definition of 'Consent' under sub-regulation 2(k) was not there in the Draft Telecom Commercial Communication Customer Preference (Third Amendment) Regulations, 2026, published on 13th March, 2026, hereinafter referred to as 'Draft Regulations', considering the comments received from the stakeholders regarding the definition of 'consent' under the Principal Regulations, the Authority is of the considered view that there is need to clarify the meaning of the 'consent' under TCCCPR, 2018.

ii. The Authority notes that the consent under the TCCCPR, 2018, is limited to the voluntary permission given by the customer to the Sender for the establishment of communication channel between the Sender and the customer so as to enable the Sender to communicate with the customer for promotional communications, as agreed to between them, and is distinct from any consent given by the customer to the Sender for the processing of his/ her personal data under the Digital Personal Data Protection Act, 2023.

iii. As far as compliance with DPDP Act, 2023 is concerned, any Sender or entity (Data Fiduciary) having the consent of the customer to possess and process the personal data of a customer (Data Principal) shall remain independently responsible for complying with the provisions of the Digital Personal Data Protection Act, 2023 and the rules made thereunder.

iv. It is to be noted that to counter the menace of unsolicited commercial communications, TCCCPR 2018 introduces an additional regulatory check in larger public interest whereby a promotional communication can be delivered to a customer who either has not disallowed such communications by exercising preferences or has specifically granted the permission to specific Sender(s) to receive the same by giving consent under this regulatory framework. In absence of TCCCPR 2018, no such check would have been employed by the Access Providers, and the Sender could have communicated with the customer using the telecom network.

v. For the purpose of sending promotional communication to the customer based on the 'consent' under TCCCPR 2018, the Sender only provides the customer's number to the Access Provider, which is actually a telecommunication identifier essential for routing and transmission of communication, and constitutes part of inherent telecom network function.

vi. In this regard, it is pertinent to refer to Section 4 read with Section 7 of the DPDP Act which provides that personal data may be processed either on the basis of consent or for certain legitimate uses. Sub-section 7(a) specifically talks about a situation where a customer (Data Principal) voluntarily provides personal data to a Sender (Data Fiduciary) and has not indicated any objection to its specified use. The illustrations accompanying Section 7(a) further clarify this position. Illustration I demonstrates that where an individual has voluntarily provided details for a particular purpose, commercial communication incidental to that purpose may be sent. Illustration II accompanying Section 7(a) emphasizes that the responsibility for determining the purpose and manner of processing of such data remains with the Data Fiduciary i.e., the Sender.

As far as role of the Access Providers is concerned, they are under regulatory obligations imposed by TCCCPR 2018 which has been framed to facilitate the prevention, detection and control of Unsolicited Commercial Communications with the help of Access Providers. The permission under the TCCCPR is intended solely for determining whether a commercial communication may be delivered to a customer. Such permission serving a telecom regulatory purpose is distinct from the consent that is obtained under the DPDP Act for the processing of personal data. The Authority notes that sub-section 17(1)(c) of the DPDP Act exempts processing of data that is necessary in the interests of the prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India. For making the

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

commercial communication, the Sender is already using the telecom identifier, and provides it to the Access Provider for setting up the communication. The same telecom identifier is being used for managing the delivery of such communication based on the permission or denial registered by the customer under the TCCCPR 2018 framework. Accordingly, such use of telecommunication identifier of the customer by the Access Provider, besides an inherent telecommunication network function, is exempt under Sub-Section17(1)(c).

vii. Based on the analysis above, the Authority also notes that the revocation of the consent by the customer under TCCCPR 2018 implies that such revocation remains limited to the withdrawal of the permission given by the customer to the Sender for establishment of communication channel between the Sender and the customer for promotional communications, and does not, by itself, amount to withdrawal of consent under the DPDP Act, 2023 to process personal data of the customer by the Sender.

viii. The distinction may be illustrated through the following example. A person 'X who wants to rent an accommodation may have provided her personal data to a real estate agent 'Y' in order for Y to find a suitable accommodation for X and inform her. Therefore, Y (Data Fiduciary) needs to process personal data of X (Data Principal) to find suitable accommodation for her. Such collection, storage and processing of data by Y shall be as per the provisions of DPDP Act, 2023. However, where customer X has additionally opted to receive the information from Y through SMS or traditional telephony, the regulatory framework under TCCCPR 2018 becomes applicable which based on the permission given by X to Y for making phone calls to her or sending SMS, enables the use of these communication channel for the delivery of information. If the customer X subsequently revokes such permission under TCCCPR 2018, only her permission to receive information from Y through phone calls or SMS is withdrawn while the processing of her personal data by Y continues independently. She may still continue to receive such information from the Sender through other means e.g. email. In case she also wants to withdraw the consent for processing of her personal data by Y entirely, she needs to do so under DPDP Act by taking up the mater directly with Y, and TCCCPR 2018 has no role to play in such revocation. Thus, the Authority notes that the revocation of permission under TCCCPR 2018 affects only the channel of communication, and does not determine whether personal data of the customer may otherwise be processed by the Sender.

ix. It is clarified that the processing and use of a customer's telecommunication identifier (such as a telephone number or other telecom identifier) by Access Providers for the purposes of routing commercial communications, carrying out regulatory pre-checks and post-checks, preventing, detecting and identifying Unsolicited Commercial Communications (UCC), investigating violations, and enforcing compliance with these regulations, is governed by the provisions of the TCCCPR and the regulatory obligations imposed thereunder. Such processing is undertaken by the Access Providers solely for the discharge of their regulation mandated functions. The rights and obligations relating to the processing of personal data by the Sender as a Data Fiduciary shall continue to be governed independently by the provisions of the Digital Personal Data Protection Act, 2023.

x. Finally, the Authority also notes that nothing contained in the regulations exempts the Sender from its obligations, or liability under the Digital Personal Data Protection Act, 2023.

3. 'Explicit consent':

A. Stakeholders' comments

a) A few stakeholders suggested that TSPs don't have any mechanism of verifying the consents. If the process 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.

b) Some of the stakeholders also suggested to consider aligning procedural guidelines on separate and specific requirements for uploading regularly on the Consent Register with other adjacent and related laws e.g.: DPDPA, IT and Evidence Act and sectoral regulations.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

c) While a few stakeholders supported the modified definition, it was suggested that the legacy consent registered under this clause shall be accompanied by an audit trail demonstrating the time, mode, and content of consent capture, and the Recipient shall be intimated of such registration within seven days, with a clear and accessible mechanism to revoke such consent.

d) Another stakeholder suggested that VNOs should be explicitly authorized to register legacy consents on behalf of their Principal Entity clients through the NSO-operated Consent Register Framework portal, using the VNO's unique Licensee ID and NSO provided access to DLT model.

B. Analysis and conclusion:

i. As per the extant regulations, "explicit consent" is defined as a consent verified directly from the recipient and recorded by the Consent Registrar. It does not include legacy consents lawfully obtained by the Senders outside the consent framework. In the absence of any provision for uploading legacy offline consents onto the digital platform, this framework did not get encouraging response from business entities since it might affect their business continuity adversely. Accordingly, to enable the recognition and digitization of legacy consents available with the entities, a revised definition of explicit consent has been introduced which recognises such legacy consents, provided they are subsequently registered in the Consent Register in accordance with the procedure specified by the Authority. This change is expected to enable orderly migration of lawfully obtained consents to the CRF ecosystem while ensuring transparency and preserving the subscriber's right to be notified and revoke such consents.

ii. As far as issue of verifying the consent is concerned, the Authority notes that the consent for receiving commercial communication is to be taken by the Sender and to be uploaded on the digital platform as per the prescribed procedure, and the customer would be able to manage this consent including its revocation any time through the prescribed mechanism. However, in case of a customer complaint where the Sender claims to have sent the commercial communication based on the customer's consent, the Originating Access Provider, as per the complaint mechanism mandated by regulation 25, has to verify the 'existence of consent' with the Sender, and such consent must, on its face, appear genuine to an objective, reasonable observer.

iii. Regarding aligning procedural guidelines with other adjacent and related laws such as DPDP Act, IT Act, Evidence Act etc, and sectoral regulations, it is noted that besides clarifying the scope of verification of consent by the Access Provider in the para above, the scope of consent has also been elaborated at para 2 above regarding amendment to the definition of consent i.e. Regulation 2(k).

iv. With regards to the comment that legacy consents registered under this clause shall be accompanied by an audit trail, and that the Recipient shall be intimated of such registration within a defined period, with a clear and accessible mechanism to revoke such consent, it is noted that the Authority vide its Direction dated 10.12.2025, has already conducted a successful pilot with 11 banks on the modified mechanism for the Consent Registration Function (CRF) to enable uploading of legacy consents by the Senders, and management of the uploaded consents by the customers. Under this mechanism, the customers receives SMS notification when their consents are uploaded on the CRF platform. The notification SMS contains a secure link directing the customer to the authorized Consent Management Page of the Telecom Service Provider (TSP) where the customer is able to view and manage the consents recorded against his/her number. In case customer wants to revoke any consents, the same can be done easily on this portal of TSP. The Authority will issue further necessary directions in this regard for smooth operation of the consent management.

v. The issues raised in relation to Virtual Network Operators VNOs are related to the availability of the access to the DLT platform for carrying out their regulation mandated functions. This has been dealt with elsewhere in the explanatory memorandum.

4. AMENDMENTS TO DEFINITIONS:

4.1 Definition of 'Message', 'Regulatory Sandbox', 'Subscriber', 'Telecom Resources' and "Unsolicited Commercial Communication (UCC)"

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

A. Stakeholders' comments

a) One stakeholder suggested that there should be minimum consumer safeguards provision within sandbox with explicit mention of scope, duration, user consent in participation etc.

b) Another stakeholder suggested to add provision of Trial period in Sandbox where entities can test their SMS templates and voice patterns in trial environment.

c) One stakeholder suggested to remove term "live" in definition as it can be done in controlled test environment under monitored conditions.

d) Regarding the amendment to the definition of 'Subscriber', two stakeholders suggested to include subscribers of App based communication services in the definition, citing the increase in spam and scam communication through these app-based communication services, and to ensure level-playing field for all stakeholders.

B. Analysis and conclusion:

i. Some of the terms used in the regulations, such as 'message', 'regulatory sandbox', 'Subscriber' and 'Telecom Resources' have been realigned with the Telecommunication Act, 2023 so as to maintain consistency between the two.

ii. The extant definition of 'message' as contained in sub-regulation 2(ai) refers to the Indian Telegraph Act,1885. The same has been amended to refer to the relevant clause and section of the Telecommunications Act, 2023.

iii. Similarly, the extant definition of 'Telecom resources' refers to any 'telegraph' used to send voice call or messages as Telecom resource. Accordingly, the same has been amended to replace 'telegraph' with "telecommunication equipment and/or telecommunication identifier", as defined under The Telecommunications Act, 2023.

iv. The amendment in the definition of "Subscriber' has also been made to maintain consistency with the Telecommunications Act, 2023.

v. In relation to the definition of "Regulatory Sandbox", regarding suggestions on providing for consumer safeguards, scope, duration, user consent in participation, trial period etc, the Authority notes that the definition of "Regulatory Sandbox" mentions that it is a live testing environment where new products, services, processes, regulatory technology solutions and business models may be deployed for a limited set of customers, for a specified period of time, with certain relaxations in the extant regulatory provisions. Accordingly, the definition already takes care of the various aspects highlighted by the stakeholders.

vi. Certain stakeholders recommended the removal of the term "live" from the definition of Regulatory Sandbox. However, the inclusion of the term is essential to the very concept and purpose of the sandbox. Removing the term "live" would confine the testing similar to lab testing and would not allow for the evaluation of services under actual operating conditions. Therefore, the term "live" has been retained in the definition to ensure that the regulatory sandbox continues to facilitate testing in actual market conditions rather than in a purely experimental environment.

4.2 Definition of '*Relationship*', *"Service message or Service Call"* and "Inferred Consent"

A. Stakeholders' comments:

a) Many stakeholders were of the view that the earlier definition of "Relationship" should be reinstated, or at least the term "inquiry" should be restored in the definition, citing various use cases. One stakeholder stated that the definition requires modification to remove the ambiguity between the seven-day validity limit of explicit consent under the definition of service calls/messages and the three-month validity period after submission of an application under the definition of Relationship.

b) It was also suggested by a stakeholder that claims of website registration or inquiry should not be accepted without verifiable consent records and auditable proof.

c) Some stakeholders suggested inclusion of specific terms such as "Digital Journey Initiation", "Expression of Interest" and "business-related enquiries" in the definition.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

d) One stakeholder submitted that removal of the phrase "on the basis of purchase or transaction" from the definition of Relationship would leave businesses without a compliant mechanism to communicate with their own customers for legitimate purposes such as renewals and continuation of services.

e) Another stakeholder suggested that while the term "inquiry" may be restored, its validity should be restricted to seven days, and such inquiries should only be made through verifiable channels to prevent misuse. One stakeholder further submitted that the validity of legacy consents should also be clearly defined.

f) A stakeholder supporting the narrower definition suggested incorporating misuse-related guardrails, specifically clarifying that the existence of a relationship should not be construed as permission to send promotional communications.

g) Another stakeholder suggested that the definition should clearly specify whether customers who disengage or drop off during a service journey may be contacted again after a cooling-off period of 7 days within the overall 3-month validity period applicable to Service Messages/Service Calls, in order to avoid ambiguity regarding permissible follow-up communications.

h) Many stakeholders commented that restriction of communication with consumers within 7 days of inquiry with consent creates ambiguity with consent obtained through CRF where validity of consent is till revocation. Definition revision should also include clarification on this ambiguity.

i) One stakeholder commented that limit of seven days to be increased to thirty days, and carving out specific 12-month timeline beyond the service-end date for specific use cases.

j) Regarding amendment to the definition of Service message or Service Call, none of the stakeholder commented on changes proposed in definitions but there was a suggestion to include in the definition a message sent or voice call made by a Sender to a recipient to respond/ fulfil business related enquiries made by him/her.

B. Analysis and conclusion:

i. Sub-regulation (bb) of regulation 2 defines "Relationship" for the purpose of inferred consent. As per its sub-clause (ii), 'Relationship' is deemed to exist on the basis of the purchase or transaction done by the recipient with the Sender within twelve months immediately preceding the date of the communication. However, under amendments to the regulations done in Feb-2025, it has been specifically provided vide first proviso to definition of 'inferred consent' (sub-regulation 2(ah)) that such consent shall not extend beyond duration / discharge of the contract between the Sender and the Recipient. In view of this amendment, the existing sub-clause (ii) from the definition of "Relationship" as provided under 2 (bb) has been removed.

ii. Further, as per sub-clause (iii) of the extant definition, 'Relationship' is deemed to exist 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.

iii. The Authority has observed that when customer complaints are received against promotional communications, many a times Senders misinterpret 'inquiry' to mean 'oral inquiry" in order to justify sending of such communications. However, such a justification is not plausible as to why a customer who has made a genuine oral inquiry to a Sender would file a complaint against the Sender. In absence of a digital or physical proof of such inquiry, it can only be concluded that either the Sender has made the commercial communication without any inquiry from the customer, or the customer has earlier terminated such relationship. Accordingly, in the draft regulations published on 13th March, 2026, it was proposed to delete the word 'inquiry" from this definition of Relationship. However, many stakeholders have suggested to retain 'inquiry' in the definition of Relationship as businesses do get genuine inquiries from the customers for goods, services etc, for which they need to communicate with the customers. Considering the legitimate need of businesses to communicate with the customers on the basis of genuine inquiries, it has been decided to retain 'inquiry' in the definition of Relationship. At the same time, to avoid any misuse of this provision for sending UCC through arbitrary interpretation of the word 'inquiry', such an inquiry must be made in writing or through digital means, and should be maintained in a verifiable form by the Sender. Moreover, it has been decided that commercial

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

communication based on such relationship should be permitted for a limited period of maximum seven days, subject to the termination of such relationship earlier by either party.

iv. Concern of another stakeholder that removal of the phrase "on the basis of purchase or transaction" from the definition of Relationship would leave businesses without a mechanism to communicate with their own customers for legitimate purposes, is also unfounded as such communications are already covered under the definition of inferred consent which, however, provides that such consent shall be limited to the duration / discharge of the contract between the Sender and the Recipient.

v. The Authority further notes that there is no ambiguity between the period of 7 days permitted for communications in relation to an 'inquiry' and 3 months period in relation to an application, since, in case of 'inquiry', the customer has only shown the interest and is only at the stage of understanding the offer while in case of application, the customer has already taken a decision and applied for the good/service etc. where much more time may be needed to complete the transaction.

vi. Regarding the comment of a stakeholder about the ambiguity between the consent provided by the customer for receiving promotional communications where validity of consent is till revocation, and the consent against an inquiry which is valid for 7 days, the Authority is of the view that period for different types of consents may be different as there are different purposes of the consents, and accordingly, consent registration function (CRF) must capture the validity of an explicit consent, wherever applicable.

vii. Since there are different periods permitted for making commercial communications by the Senders on the basis of relationship i.e. 7 days in case of inquiry and 3 months in case of application as contained in the definition of 'Relationship", and, the period of contract in case of transaction as contained in the definition of "Inferred Consent', the Authority notes that to bring more clarity, the first proviso to the definition of 'Inferred Consent' in clause 2 (ah) which provides the permitted time limit for commercial communications in case of transaction, needs to be deleted from the definition of 'Inferred Consent', and to be inserted as proviso to the first sub-clause of the definition of "Relationship" so that various time limits appear under the same definition.

viii. The Authority also notes that as per the extant sub-clause (iv) of the definition, 'Relationship' is deemed to exist 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. It is felt that such communication is not of the nature of commercial communication, as defined under regulations vide sub-regulation 2(i). It is, accordingly, decided to remove this sub-clause to avoid any misuse by Senders for sending UCC in the garb of communications being sent for social reasons.

ix. Further, in the extant definition of 'Service message or Service Call', inadvertently, only 'message' was mentioned at few places instead of 'messages or voice calls'. Accordingly, the same has been corrected. The Authority also notes that Authentication OTPs are sent to customers not only in case of transactions but also in relation to services e.g. App login, password reset, two-factor authentication etc. Therefore, messages containing OTPs for such purposes constitute service messages. It was noted by the Authority that the "OTPs for apps login" were inadvertently mentioned in the definition of 'Transactional messages". Accordingly, the reference to such OTPs has been removed from the category of Transactional messages and included in the definition of Service message.

x. Besides, the first proviso has been amended and additional proviso has been introduced in the sub-clause (ii) of sub-regulation 2(bh) to provide that explicit consent for service message or call under the aforesaid sub-clause may be renewed for an additional period of seven days at a time, if customer needs more time and desires so; and that the Authority may specify the validity period of such explicit consent from time to time so as to meet the dynamic requirements of the ecosystem.

4.3 New terms: 'Spam' and 'Spammer'

i. The Authority has introduced the definition of 'Spam' and 'Spammer' in the regulations as these terms are commonly used by the customers to mean UCC and UCC Sender/TM, respectively. At the same time, these terms are also used by customers sometimes to mean fraudulent communications and fraudsters, respectively. Therefore, it has been decided to introduce these terms into regulatory framework, clearly

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

defining their scope as far as TCCCPR 2018 is concerned. Accordingly, "Spam" has been defined to mean 'Unsolicited Commercial Communication' and "Spammer" has been defined to mean a Sender or Telemarketer engaged in sending Unsolicited Commercial Communication (UCC) for the purpose of these regulations.

5. **A2P Calls:**

A. **Stakeholders' comments on the definition of A2P calls**

a) Many stakeholders submitted that a voice call may not be classified as an A2P call if a live human agent is directly and actively participating as a party in the call, even if the call is initiated through an API, automated platform, or CPaaS system. Some of the examples cited include ride-hailing platforms where the app connects a live driver to the customer, delivery coordination calls, healthcare teleconsultation bridging for connecting doctor to patient, enterprise customer support via agent dialer. It was submitted that in all such cases, the API merely facilitates the connections analogous to a telephone exchange and that these are not robo-calls or prerecorded messages. Subjecting them to A2P termination charges and the pre-declaration regime will impose enormous cost and compliance burden on legitimate transactional services without any UCC prevention benefit. A precise definition is essential before the charge and compliance regime is operationalized. Another stakeholder submitted that the use of autodialing or similar technologies shall not, by itself, be determinative of A2P classification, as this technology may also be used for human-initiated calls in the ordinary course of communication.

b) One Stakeholder submitted that there may not be a requirement to introduce a separate definition of "A2P Calls" within the TCCCP Regulations. The Regulations already define "Commercial Communication" which adequately encompasses all forms of commercial interactions, including both Application-to-Person (A2P) and Person-to-Person (P2P) communications. With the increasing convergence of communication technologies, including the use of enterprise communication platforms, the distinction between A2P and P2P calls becomes blurred and difficult to enforce from a network and compliance standpoint. The inclusion of A2P as a distinct category may result in ambiguity in interpretation.

c) One stakeholder submitted that the definition of A2P calls is agreed, however, the information whether the customer i.e. the Sender, is going to use the service for manual dialling or auto dialling, be it LL, SIP/PRI, FTTH, Mobile, VoIP etc., is not available as on now.

d) Another stakeholder stated that there is no requirement of such definition as it may not accurately capture the intended scope of commercial communications and may lead to inconsistencies in implementation across TSPs.

B. **Stakeholders' comments on pre-declaration of A2P calls with OAPs**

a) Many stakeholders suggested that pre-declaration of A2P calls should be carried out on the DLT system in a standardized format containing details such as CLI range, intended objective, expected call volume, and details of intermediaries, without which enforcement may become difficult.

b) It was commented by a stakeholder that clear guidelines are required for identification of A2P calls where no prior declaration exists, particularly for agent assisted or AI-enabled interactions, to avoid ambiguity at the TSP level.

c) One stakeholder suggested that such declaration requirements should apply only to A2P commercial calls and not to all A2P calls.

d) Another stakeholder commented that Agent-Assisted calls, AI-enabled calls, customer-requested callback calls, and calls initiated through AI/IVR with subsequent handover to human agents should be excluded from A2P declaration requirements.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

e) One stakeholder cited technical and operational challenges in declaration of A2P calls where a VNO acts as an intermediary, while another stakeholder submitted that action for non-compliance should be taken against the Principal Entity instead of the CLI, as the CLI may at times be owned by an intermediary.

f) One stakeholder suggested that, after declaration, A2P calls may be tagged as "Verified Business" or "Suspected Spam" in the caller ID. Another stakeholder suggested incorporating aggravated consequences for intentional non-declaration, misdeclaration, and repeated instances of misdeclaration.

g) One stakeholder further suggested that the levels/categories applicable to A2P calls should be pre-declared for all stakeholders for billing purposes.

C. Stakeholders' comments on Deterrent charges

a) Some stakeholders submitted that all commercial communication calls i.e. all Promotional, Transactional, and Service Calls, irrespective of the method or platform used for origination should also be considered A2P calls.

b) One stakeholder submitted that exemptions should be broadened to cover entities outside existing designated numbering frameworks, and the imposition of A2P termination charges should be deferred until a comprehensive numbering framework is established, with all designated numbering series and bona fide service and transactional A2P calls remaining exempt from such charges.

c) Other stakeholders suggested that this clause should be deleted as it imposes additional cost burden on legitimate and compliant A2P communications, and may act as a significant deterrent to critical transactional communications such as voice-based OTPs and payment alerts. Telecom charging principles have traditionally been based on the "work done" by the network. A2P calls do not impose any incremental cost on the network vis-à-vis other voice calls. Imposition of such charges may lead to market distortions, including migration of traffic to alternate platforms outside the regulatory framework, thereby potentially undermining the very objective of ensuring traceability and control over commercial communications.

d) One stakeholder submitted that there is lack of technical mechanism for traffic segregation. Without a clear, mandated segregation protocol, including A2P charges will trigger frequent billing disputes between the Originating Access Provider (OAP) and the Terminating Access Provider (TAP), as each may classify the same traffic differently.

e) One of the stakeholders submitted that this will create "perverse incentive" for enterprise customers to misrepresent their usage as standard P2P to secure lower rates. Accordingly, the rate be fixed at exactly ₹0.05 or any other rate as decided by Authority, and "not upto" for A2P calls and SMS.

f) Few stakeholders suggested that TAP may be allowed to charge OAP up to 50p/minute instead of 5p/minutes. TAP may also be allowed to charge OAP up to 5p for each call attempt in case of commercial calls including A2P and P2P calls. Provided that there shall be no termination charge or attempt-based charging on government communication.

g) Few stakeholders suggested that there will be structural advantage for large Terminating Access Providers (TAPs) as the proposed framework permits only TAPs to levy termination charges. Operators with a large subscriber base may benefit through higher Terminating traffic volumes and on-net traffic advantages. Therefore, there is a risk of traffic diversion instead of UCC reduction as it may shift the traffic towards operators with stronger on-net advantages. It was suggested to apply deterrent measures at OAP-end, and instead of termination charges, a floor tariff or separate tariff based on slab of volume of calls, for the commercial communications voice calls may be prescribed as a deterrent.

h) It was commented that the commercials are a matter of contract and should be agreed between parties mutually. Such charges should not be made part of the regulation and left to be decided by market participants.

i) It was also commented to exempt A2P Charges for VNOs as VNOs have bilateral one-to-one commercial agreements with TSPs, and cost recovery is already governed by the commercial contracts. A regulatory charge creates a "double-tax" on AGR-paying entities.

j) The Authority should not make commercial communication charge as Nil (zero) for Govt exempted headers (except for disaster management). The inter-operator commercial SMS communication charge for such

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

messages should not be made Nil and can be at a reduced price i.e. Rs 0.02 per SMS besides Rs 0.02/SMS IUC.

k) One TSP suggested to increase the charges to Rs 0.10 (ten paise only) or Rs. 0.11 (eleven paise only) for SMS and claimed that the present ₹0.05 additional component was not designed as a deterrent, but rather as a commercial construct to support regulatory processes.

D. Analysis and conclusion:

i. Application-to-Person (A2P) calling is being used for bulk commercial communications due to its ability to automate and scale large volumes of calls. While these features make it useful for legitimate business purposes, they have also led to widespread misuse, resulting in nuisance and unsolicited commercial communications to the consumers. Considering these characteristics of A2P voice calls, the regulatory framework needs to address any regulatory gaps which may be exploited for transmitting unsolicited commercial communications.

ii. The Authority notes that the compliance data furnished by the Access Providers indicates that a substantial proportion of violations relating to commercial communications are associated with enterprise communication resources i.e. A2P calls. During April 2026, out of the total 20,591 disconnections, 15,736 SIP/PRI connections (used for A2P calls) were disconnected, accounting for approximately 75% of the total disconnections undertaken in respect of such violations. The aforesaid data necessitates the introduction of appropriate regulatory measures for A2P calling so as to prevent the misuse of such platforms for sending UCC.

iii. Many stakeholders have suggested that definition of A2P may exclude those where there is live human agent. However, it is observed that it will be technically not feasible for the Access Providers to identify in which case there is human agent participating in the A2P, and in which case it is not. In any case A2P calling from designated series is exempted from such termination charge. Hence Authority is of the view that there is no necessity of any change in proposed definition of A2P calls. Regarding the comment of a stakeholder that there may not be a requirement to introduce a separate definition of "A2P Calls" within the TCCCP Regulations as the same is covered under the definition of 'commercial communications', the Authority notes that the definition of "A2P Calls" under the amendments is based on technical aspects of the call generation while that of 'commercial communications' is based on the nature of the content being communicated. Accordingly, keeping in view the prime objective of preventing UCC that can be generated at large scale using the A2P platforms, there is a need to define A2P call in the regulation.

iv. As far as identification of A2P calls for the purpose of imposing termination charges is concerned, presently it appears technically challenging to differentiate such calling from P2P calling as telecom network may not be able to differentiate between the A2P call and P2P call, between voice of an actual human interacting on call and a pre-recorded or artificially generated human voice. Therefore, the bulk callers must pre-declare to the OAP, the use of A2P calling along with the details such as CLI ranges to be used for making A2P calls, or any other details as specified by the Authority from time to time, and such declaration should be recorded on the DLT platform so as to have transparency about such calling. In case, the bulk caller fails to declare use of A2P calling, and is detected so upon investigation/inspection, all such calls shall be treated as UCC, and action shall be taken by the Access Providers as per the regulatory provisions. Declaration of enterprise identity is not considered necessary at this stage as CLI range itself should be able to identify such calling on the network.

v. Regarding the comment that such declaration requirements should apply only to A2P commercial calls and not to all A2P calls, the Authority notes that as A2P calling is used for making bulk communication, the regulations apply to all A2P calls. Otherwise, limiting the scope of A2P calls to be covered under regulations may result in regulatory arbitrage, leading to misuse of A2P calling for sending UCC in the garb of transaction or service calling. Moreover, the Authority is of the opinion that it would practically difficult to distinguish whether an A2P call made from numbers other than designated series was used for commercial and non-commercial communication.

vi. On the suggestion of one of the stakeholders that action for non-compliance should be taken against the Principal Entity instead of the CLI, as the CLI may at times be owned by an intermediary, it is to be noted that under the regulatory framework, action for non-compliance is taken by the Access Provider against the telecom resources

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

of the Sender. Therefore, in case the CLIs owned by an intermediary are used by a PE for sending UCC, the intermediary must ensure that such CLIs are not misused for UCC, otherwise, action under the regulation will be taken by the Access Providers against the telecom resources of the intermediary, without prejudice to any other regulatory action that may be taken against the PE.

vii. One of the factors contributing to the misuse of A2P calling for unregistered telemarketing is the absence of any additional charges for A2P calling e.g. termination charges, that can act as a deterrent against such misuse. The bulk callers take advantage of cheaper routes meant for normal person-to-person (P2P) calls, and misuse them for unsolicited A2P commercial calling. Accordingly, it is necessary to have a deterrent in the form of inter-operator charge, since A2P calls are made in bulk at the OAP end and passed onto the network of the TAP.

viii. Although another possible alternative is the imposition of higher tariff at OAP end for such calling however taking into account the fact that an OAP has direct business interest in origination of such calls, the A2P callers may be able to get substantially discounted rates. Hence, there exists a conflict of interest.

ix. It may be noted that the extant regulations already provide for an inter-operator charge upto Rs. 0.05 (five paisa only) as a deterrent for each commercial SMS. Accordingly, at this stage, a charge of upto Rs 0.05(five paisa only is considered a good base for introduction of this charge as of now for termination of A2P calls. Further, the charge of upto ₹0.05 per call is intended solely as a deterrent measure and not as a cost-recovery mechanism. The recovery of regulatory and operational costs is taken care under the interconnection framework governed under the licensing/authorisation conditions and relevant regulatory provisions. Since this is the first time such a charge for A2P voice calls has been introduced, an amount analogous to commercial SMS has been prescribed instead of prescribing a higher amount as suggested by some stakeholders. The more important aspect is to encourage compliance without unreasonable burden on stakeholders. The effectiveness of the prescribed charge will be reviewed, and any modification, if required, may be considered based on the experience gained from its implementation.

x. The Authority appreciates the concern raised by some of the stakeholders that due to structural advantage for large Terminating Access Providers (TAPs), smaller Access Providers who primarily function as OAP, may face competitive disadvantage. In the commercial communication ecosystem, the TAP controls inter-operator charge, which is a key input for competing TSPs in downstream markets. There may arise a situation where the larger TAPs may keep inter-operator charge higher than the price for a Sender directly connected with it, which can have substantial impact on the smaller Access Providers in terms of reduction or elimination of the profits, and making them non-competitive in the market. As the inter-operator charge for commercial communication is regulated under the TCCCP Regulations, the Authority has considered it crucial to put guardrails so that the inter-operator charge is not used as a mechanism of vertical squeeze for unfairly limiting the competition. Accordingly, the Authority has mandated that the TAP shall not take from the OAP such charge which is more than the lowest tariff offered by the Terminating Access Provider to the Senders/ Telemarketers who are directly connected with them i.e. for whom it acts as the Originating Access Provider. Such a provision has been incorporated for both A2P calls (Regulation 35A) as well as SMS (Regulation 35) to prevent any competitive disadvantage to the smaller OAPs. Further, regarding the suggestion of a stakeholder that the rate be fixed at exactly ₹0.05 or any other rate as decided by Authority, and "not upto" for A2P calls and SMS to avoid 'perverse incentive" for enterprise customers to misrepresent their usage as standard P2P to secure lower rates, it is noted that the Authority prescribes the ceiling rates leaving actual rate determination upto market forces, and does not find merit in the comment made by the stakeholder as such perceived perverse incentives are not going to be affected by fixed rate either.

xi. Regarding certain comments of the stakeholders that commercials are a matter of contract and should be agreed between parties mutually, and exempting A2P Charges for VNOs as VNOs have bilateral one-to-one commercial agreements with TSPs, it has already been noted that the charge prescribed under Regulation 35 and 35A is intended solely as a deterrent measure and not as a cost-recovery mechanism or commercial charge.

xii. Regulation 3 of the regulations mandates sending commercial communication, including A2P calls, using only registered headers or the number resources allotted to the Senders from special series assigned for the purpose of

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

commercial communication. Accordingly, 140xx series has already been mandated for promotional calls by all the registered Senders and Telemarketers, 1600xx series has been mandated for service and transactional calls by the entities in the BFSI sectors, and for Government to citizen communications, and 1601xx numbering series for Service and Transactional Voice Calls by entities in sectors other than BFSI and Government sector. Since the commercial calls being made by the registered Senders/ Telemarketers using number resources assigned from the series designated by the Authority such as 140xx series, 1600xx and 1601xx series, have to be made in accordance with the regulatory provisions, and any violation of the same by the RTMs has to be dealt with as per the provisions of TCCCPR, 2018, only, the A2P calling using such number resources has also been exempted from the termination charges. Also, one of the key objectives of the exemption is to facilitate and incentivize the migration of Principal Entities and Telemarketers from the UTM framework to the RTM framework. Such migration is expected to enhance accountability, improve traceability of commercial communications, and strengthen regulatory oversight. Further, the A2P calls by Government for which 1600 Series has been designated and calls by the Authority or any agency authorized by the Authority are made in the larger public interest for purposes such as public safety alerts, information and updates on welfare schemes, cyber security alerts, consumer awareness campaigns, emergency notifications etc., these communications are non-commercial in nature and are meant for citizen awareness and protection. Exempting them from termination charges ensures that critical information can be delivered widely without cost constraints.

xiii. Regarding the comment of a few stakeholders to exempt legitimate transactional and service communications by broadening the exemptions to cover entities outside existing designated numbering series through declaration of their calling numbers on DLT platform, the Authority is of the opinion that considering the key aspects of ease of technical implementation as well as easier identification of the commercial communications by the recipients, designating special series for commercial communications would be the appropriate approach. Besides 140xx and 1600xx, 1601xx series, the Authority may designate special series for service, transactional or government communications from time to time, and also examine whether to exempt such series from termination charges applicable to A2P calls.

xiv. However, as suggested by some stakeholders, to ensure visibility of numbers being used to make A2P calls, and enable proper billing by the TAP, it is necessary that OAP shall specify on DLT platform the numbering resources/series/levels assigned to Sender for A2P calls.

6. Classification of Senders for the purpose of making commercial communication using registered headers or special series

A. Stakeholders' Comments:

a) It was commented to specify industry-wise and use-case-based classifications, such as logistics, banking, healthcare, OTPs, and service communications, along with clear criteria for determining criticality, to avoid ambiguity.

b) A few stakeholders submitted that such classification should be based on a risk-based Sender taxonomy with published criteria and corresponding consequence bands. It was further suggested that all classes should continue to support baseline consumer privacy and choice protections.

c) A few stakeholders specifically referred to certain sectors for which criteria should be defined, while some stakeholders submitted that entities such as VNOs (Virtual Network Operators) and Registered Cloud Communication Platforms (RCCPs) should be recognized as distinct entities for which separate criteria may be prescribed, considering their specific role in the ecosystem.

d) One stakeholder further submitted that differentiated criteria should be introduced with respect to specific reference to registration, declaration, complaint thresholds, and enforcement mechanisms.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

e) A few stakeholders suggested the expansion of the 1600-series or equivalent differentiated treatment/protection framework to legitimate transactional and service communications across non-BFSI sectors. such as healthcare, logistics, e-commerce, education, travel, telecom etc., along with interim safeguards against AI-flagging, complaint thresholds and enforcement actions for verified Senders.

f) Some stakeholders suggested that any such classification of Senders should be undertaken only after consultation with TSPs to assess operational and technical feasibility and to preserve the spirit of the co-regulatory framework.

g) Some of the stakeholders submitted that highly granular Sender classification may be technically and operationally difficult for TSPs and requested the Authority to explicitly notify Enterprise and Government entities along with clearly defined differentiated enforcement criteria with the amendment itself.

B. Analysis and Conclusion:

i. TRAI has mandated use of 140xx series for promotional calls while use of 1600 series numbers have been mandated for making transactional and service calls by the BFSI sector entities and for government to citizen communications. During various interaction with Access Providers, and as also noted from the comments of the stakeholders, there are suggestions for designating special series for covering legitimate transactional and service communication from other sectors also or extending 1600 series itself to such communications.

ii. However, it emerged during deliberations with sectoral regulators as well as Access Providers that considering the importance of government and financial communications for the citizens, it is not desirable to extend 1600 series to other sectors, and instead separate series may be issued for them. Accordingly, a separate 1601xx series has been recently allotted by the Department of Telecommunications for transactional and service calls by other sectors. The Authority plans to introduce this series in a phased manner and has issued a Direction on 10th August, 2026 for first phase of its operationalisation, covering Utilities, Logistics and Courier services.

iii. Another important aspect that emerged out of deliberations with sectoral regulators is that even within BFSI sector, it may not be desirable to mandate 1600 series numbers for all the entities in the BFSI sector as many small players work on a limited scale, interacting with only a few customers with whom they already have existing relationship. It was suggested that such small players may be exempted from mandatorily using 1600 series numbers, and in case they try to misuse the exemption, action may be taken against them treating such communication as UCC from UTMs. However, they may be permitted to optionally use 1600 numbers.

iv. In view of the above, the first proviso introduced to sub-regulation (1) of regulation 3 of the *Regulations* enables the Authority to classify Senders and specify different criteria for different classes of Senders, including exempting certain classes of Senders, if deemed necessary.

v. Regarding the comments of stakeholders to have clear criteria for differentiation, and that such classification should be undertaken only after consultation with TSPs, the Authority notes that as the principles have already been established through the open consultation with the stakeholders, there in no need for any further consultation, and necessary directions shall be issued by Authority from time to time as deemed appropriate.

vi. As far as classifying the VNOs and Cloud Communication platforms as distinct classes of Senders, is concerned, the Authority notes that VNOs fall under the definitions of Access Providers as per sub-regulation 2(b) while the issue in relation to Cloud Communication platforms has been dealt with separately elsewhere in the explanatory memorandum.

7. Removal of provision for putting telecom resources under usage cap: Amendment to Regulation 11

A. Stakeholders' Comments:

a) It was suggested that deletion of the "usage cap" provision should not restrict the imposition of proportionate and evidence-based interim usage caps/throttling measures against suspected spam/UCC, subject to mandatory notice and review within fixed hours/days.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

b) Some of the stakeholders proposed retention of the "usage cap" provision, as industry proposals to the Authority relating to AI/ML-based spam flagging and containment mechanisms rely on such measures for effective implementation.

B. Analysis and Conclusion:

1. Regarding the comments about retaining the "usage cap" provision for the purpose of taking proportionate action against UCC, the Authority notes that the provisions for putting usage cap on the telecom resources of the Senders and Telemarketers for violation of regulations were removed by the 2025 Amendment. The Authority, vide para 56 of the explanatory memorandum to the aforesaid amendment, observed that sufficient strict actions are not in place to curb UCC from unregistered Senders/Unsolicited Telemarketing Messages (UTMs), and that the implementation of usage caps has been found to be unfeasible and difficult to monitor by the regulator. The Authority, accordingly, decided to remove the provision for putting usage cap, citing that stricter provisions are required to curb UCC from UTMs. In view of the above, the reference in sub regulation (4) of regulation 11 has been rendered redundant which has led to deletion of the words "put under usage cap or his telecom resources may be" in the aforesaid sub-regulation.
2. As far as proposal of industry relating to AI/ML-based spam flagging and containment mechanisms based on measures like usage cap is concerned, the Authority notes that detailed mechanism in relation to regulatory action to be taken against suspected Senders of UCC, based on AI/ML-based spam flagging, has already been specified under the Direction dated 27.02.2026 for institutionalisation of AI/ML-based UCC_Detect intelligence, and now incorporated as Regulation 21A under this amendment. The mechanisms specified under these regulatory measures do not include "usage cap" as an enforcement action. The term "usage cap" has, accordingly, been rendered redundant.

8. Leveraging AI to control UCC.

A. Stakeholders' Comments:

a) Some of the TSPs submitted that the relevant clauses may either be removed or suitably realigned in line with an operationally feasible approach evolved through industry consensus. It was also submitted that sending notifications to Senders immediately after AI-based flagging may alert spammers, thereby enabling them to modify their patterns to evade detection. A few stakeholders submitted that notifications served to Senders following AI-based flagging should incorporate principles of AI governance and explainability, including disclosure of the basis of flagging such as volume, velocity, diversity, or other triggering parameters.

b) Several TSPs suggested that AI-based flagging should be carried out on the basis of confidence scores while other stakeholders suggested that such mechanism should be standardized across all Access Providers on the basis of common set of parameters and the criteria for classification of confidence scores.

c) Several stakeholders raised concerns about the false positives flagged by AI systems and action taken against the Senders based on such false positives, which may cause panic among the Senders, and likely surge in customer queries to call centres of TSPs, with users seeking explanations for flagging and requesting its removal, and that this will impact call centres KPIs. It was also submitted that as AI/ML-based systems rely on behavioural patterns, there exists a significant possibility that the calling patterns of genuine call centres may resemble those of robo-callers.

d) It was also suggested to establish a governance and escalation framework for addressing false positive cases. A few stakeholders also suggested that all AI-generated outputs should mandatorily undergo human review before initiation of any deterrent action, thereby acting as a safeguard against false positives.

e) Many stakeholders suggested incorporation of provisions relating to whitelisting of genuine business entities to prevent unwarranted flagging by AI/ML systems. They also suggested development of a mechanism enabling Principal Entities to challenge or appeal against flagging by AI/ML-based systems. One stakeholder suggested

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

that, for aggregator businesses, pre-registration of CLI on the DLT platform along with the purpose of calling should be mandated.

f) One stakeholder suggested automatic whitelisting of Senders upon successful completion of re-KYC, while another stakeholder proposed the use of volume-based triggers prior to complaint-based triggers in AI-driven flagging systems.

g) Further, these stakeholders stated that re-KYC and physical verification disproportionately impact genuine and legitimate users more than spammers, and that such measures are not specifically mandated under existing license conditions.

h) Another issue emerging from stakeholder comments related to the safeguards required while sharing KYC identifiers among operators. Stakeholders emphasized the need for minimum privacy and security baselines.

i) One stakeholder suggested that action in cases of failed re-KYC should be differentiated from cases where Senders are found to be misusing telecom resources for UCC activities.

j) Another stakeholder suggested that no additional KYC requirement should be imposed on enterprise customers, as periodic KYC is already undertaken in compliance with license conditions.

k) One stakeholder suggested that the AI/ML-based systems deployed by TSPs should first be tested extensively with the banking industry for a period of six months prior to wider implementation.

l) In addition, one stakeholder suggested that promotional complaints should be shared with Senders for response or investigation only after analysis of call recordings. Another stakeholder suggested that throttling or blocking of spammers immediately after flagging may serve as an effective preventive measure for spam control.

m) Regarding introduction of an additional reduced complaint threshold based on corroboration with AI based flagging under Regulation 25, it was suggested by another stakeholder that the threshold for triggering action should not be reduced below five complaints, and that only complaints decided in favour of consumers should be considered for enforcement.

B. <u>Analysis and Conclusion:</u>

i. Under the present regulations, the action against the UCC Sender is triggered when there are '5 or more complaints against the Sender from unique recipients in last 10 days' i.e. primarily it is complaint-based mechanism. However, the Authority has observed that majority of UCC complaints are reported against Unregistered Telemarketers (UTMs). For the period from Jan'26 to Apr'26, a total of 11,49,186 UCC complaints were received by the Access Providers, out of which 10,26,187 complaints i.e. 89.3%, were against the Unregistered Telemarketers (UTMs). Such communications typically bypass the DND registry and other controls available on the DLT platform, thereby limiting the effectiveness of a purely complaint-driven enforcement mechanism. Further, under the present framework, a large number of complaints do not ultimately qualify for regulatory action owing to the prescribed thresholds, resulting in delayed intervention against persistent offenders.

ii. Presently, major Access Providers have deployed AI/ML-based systems in accordance with Schedule IV of the Regulations for detection of suspected spam communications. As per the data furnished by the Access Providers, AI systems have been flagging a substantial number of calls and messages as suspected spam communications for alerting the recipients. For the month of April-2026, these AI systems flagged, on an average, more than 25 Crore calls per day and 1.6 crore SMS per day as suspected spam. However, these systems are largely being used for generating subscriber-facing alerts only. While such alerting help subscribers exercise caution, it does not act as an effective deterrent against UCC Senders as no action is being taken against them. Consequently,

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

enforcement has continued to remain predominantly complaint-driven despite the demonstrated effectiveness of AI/ML-based detection systems.

iii. Recognising the potential of these technological tools for effectively controlling UCC, the Authority issued a Direction on 27.02.2026 for institutionalisation of AI/ML-based UCC_Detect intelligence for inter-operator sharing and for further investigation of such suspect Senders. The action is required to be taken by the Access Providers based on the result of investigation. Accordingly, The Direction requires Access Providers to undertake re-verification of KYC documents of suspected UCC Sender whenever the threshold criterion defined in the Direction is met, and action is required to be taken as per KYC guidelines of DoT. In case of repetition of such activity, the Direction mandates the Access Providers to carry out the physical verification of the Sender. If physical KYC verification fails or it is found that the telecom resources are being misused by the Sender for sending UCC, action against the telecom resources allotted to the Sender shall be taken by the Access Provider, as per the Direction. The new regulation 21A provides for these provisions as part of the TCCCPR 2018 regulations.

iv. The Authority also notes the suggestions of some of the stakeholders that to reduce false positives, AI-based flagging should be carried out on the basis of confidence scores and common set of parameters including criteria for classification of confidence scores across all Access Providers. Therefore, it has been decided that as far as identification of a Sender for the purpose of enforcement is concerned, such identification should be done where the probability that the Sender is engaged in sending UCC, is high, and the CLIs of such Senders should be identified as "Suspected high probability UCC CLI". Accordingly, while the flagging of CLIs suspected of sending UCC for the purpose of alerting the customers shall continue as per the algorithm of the respective service provider, sharing of such flagged CLIs and action to be taken against Senders by the Access Provider shall be limited only to suspected high probability UCC Senders. Moreover, to have consistency and effectiveness of the implementation, the Authority may specify the parameters for identifying and flagging the Calling Line Identification (CLI) of the Sender as "Suspected high probability UCC CLI" from time to time. Besides, the sharing of data of such Senders has been mandated through DLT platform. However, based on the technical considerations, the Authority may specify any other mechanism for sharing the information among the Access Providers from time to time.

v. The Authority notes that while identification of the high probability suspected Senders would significantly reduce the chances of action against false positive Senders, nevertheless, false positive may still occur. Therefore, to address this issue, Access Providers must provide a mechanism to the Senders whose CLIs have been flagged as suspected of sending UCC to represent their case with justification against the flagging, and should unflag the CLIs if justification is found in order.

vi. Also considering the fact that special series such as 140, 1600 and 1601 for commercial communications have been designated by the Authority for specific purposes and that the regulatory framework itself provides the necessary measures to check any misuse, the CLIs from 140xx series, 1600xx series, 1601xx series, or any other numbering series specially designated by the Authority for commercial communications and notified for this purpose, shall not be flagged as "Suspected UCC/spam" for the recipients. Otherwise, the customers may miss commercial communications important to them. For detailed discussion on this aspect, the analysis done with respect to regulation 34A may be referred to.

vii. Further, under the existing framework, regulatory action is triggered only when five or more complaints are received against a Sender from unique recipients within a period of ten days. An analysis of the complaint data for the month of April, 2026 indicates that, out of the 2,66,105 no. of total UCC complaints received, only 17,401 number of complaints met the prescribed threshold, covering only 1,713 number of Senders. Accordingly, the regulatory action was initiated only in respect of such cases.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

viii. However, to make an assessment of the gap that may exists between the UCC activity and the UCC complaints, the Authority, based on the data provided by the Access Providers for the month of April-2026, noticed that while about 771 Crore calls and 48 crore SMS were flagged as suspected spam by the AI systems during the said period, the number of customer complaints are only 2,66,105, out of which only 17,401 complaints could meet the threshold criteria. The analysis points to the existence of a potential gap between the UCC activity being carried out by the spammers and its reporting by the customers.

ix. Therefore, in order to improve the enforcement mechanism for enabling faster action on a wider scale against the UCC Senders, the Authority further analysed complaint data on the basis of a threshold of three or more complaints from unique recipients within ten days. The analysis indicates that 28,135 number of complaints (60% more) would meet this threshold, and would cover 6,762 number of Senders (approx. 300% more). Taking into account that the AI based flagging of suspected UCC Senders on the basis of high probability is a strong indicator of UCC activity, the Authority is of considered view that a combination of lower complaint threshold in corroboration with AI/ML-based UCC_Detect intelligence indicating suspected spam activity by the Sender with high probability during the same period, would constitute an appropriate trigger for initiating action in accordance with the regulatory framework. This amendment supplements the complaint-based mechanism with AI based technological intelligence. By corroborating the customer complaints with AI/ML-based UCC_Detect outputs, the Authority seeks to enable earlier identification of suspected high probability UCC Senders, facilitate timely investigation, minimise the risk of false positives, and strengthen enforcement against spam communications. This approach is expected to significantly enhance the effectiveness of measures aimed at curbing unsolicited commercial communications.

x. Accordingly, Regulation 25 has been amended to include an additional criterion of a reduced complaint threshold of '3 or more complaints against the Sender from unique recipients in last 10 days' if any CLI allotted to the Sender has been identified or maintained as "Suspected high probability UCC CLI" by the AI system of the Access Providers during these last ten days.

xi. It is clear from the above that the apprehension of some of the stakeholders about any action against the Senders based solely on the basis of AI based flagging or on the basis of false positives is misplaced. The Authority recognises that AI-generated intelligence, although a strong indicator of UCC activity, by itself, may not constitute conclusive evidence for enforcement action as the possibility of false positives cannot be entirely ruled out. Therefore, the regulation does not provide for treating AI-based flagging as a self-sufficient basis for regulatory action. The AI-based flagging only acts as a trigger for further investigation into the cases of suspected UCC, and regulatory action is only initiated based on the findings of the investigations as provided for in regulation 21A. Similarly, AI intelligence is to be used for corroboration with complaint data for initiating action at a lower threshold under amended regulation 25. In respect of one of the stakeholder's suggestion that there should be a human review before initiation of any deterrent action, the above explanation clarifies that there is no such need as no deterrent action is going to be taken solely based on AI intelligence.

xii. Regarding comments about alerting the spammers, the notifications will be sent only to those suspected Senders who get filtered on the basis of common parameters and high confidence score employed by the AI systems. Further, the notifications besides serving as an intimation of identification, will act as a clear message to the UCC Senders that they are being monitored and liable for action in case non-compliance by them is confirmed, thereby, warning them to refrain from sending UCC. Further, some of the stakeholders suggested that the notification must disclose the basis of flagging, and the Authority may also specify the format and manner of sending such notification from time to time, if needed. The Authority notes as the AI-flagging is done on the basis of behavioural patterns of calling and messaging, the notification will contain appropriate message to this effect. So far as surge in calls at customer care centres is concerned, in absence of any data, it is premature and presumptive to say so. However, any perceived increase in complaints can be suitably handled including by measures such as

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

properly training the call agents to give crisp reply to the callers as the cases are expected to fall in limited categories, and use appropriate standardised replies in routine cases, augmenting the capacity, etc. Further, the TCCCPR 2018 also mandates the Access Providers to undertake awareness campaigns for the users of telecommunication services, which include both recipients as well as Senders This issue is also to be seen in light of the fact that based on the data for the period from Jan-2026 to April-2026, on an average, about 250 crore commercial messages were sent per day and about 15 Crore calls from140 series numbers have been made through telecom network daily during this period. Besides this, a large number of service and transaction calls are also made by the Senders using normal 10 digit numbers. Therefore, while commercial communications are a big source of revenue for the Access Providers, there also exists a corresponding responsibility of the Access Providers to protect consumers from UCC. Accordingly, necessary arrangements need to be made by the Access Providers to comply with the regulatory mandate.

xiii. Another apprehension was raised by some of the stakeholders that some of genuine callers such as call centres or large enterprises, may suffer since there calling pattern resembles that of the UCC Senders. In this regard, it has been already discussed above that the regulations do not provide for any action against the Sender solely on the basis of AI-based intelligence. Such intelligence is to be used either as a trigger for further investigation or to be corroborated with the complaints. Therefore, there is no cause of concern for genuine users. Additionally, second proviso to sub-regulation (a) of regulation 21A has been introduced to mandate that CLI from any numbering series specially designated by the Authority for commercial communications shall not be flagged as "Suspected UCC CLI". As of now, the Authority has designated 140xx for promotional communications, 1600xx series for Government communications, and for service and transactional calls by BFSI sector entities; and 1601xx series for service and transactional calls by Utilities, Logistics and Courier companies.

xiv. Many stakeholders have suggested to have a mechanism for whitelisting of genuine business entities to prevent unwarranted flagging by AI/ML systems, and also to challenge or appeal against flagging by AI/ML-based systems. In this regard, third proviso to sub-regulation (a) of regulation 21A has been introduced which mandates the Access Providers to provide a mechanism to the flagged Senders to represent their case with justification against the flagging, and to unflag their CLIs if justification is found in order. If felt necessary, the Authority may also prescribe such mechanism from time to time. As far as whitelisting of business entities is concerned, it is felt that the same would be possible through specially designated series, considering the key advantages of using special series, which include ease of technical implementation as well as easier identification by the recipients.

xv. Some of the stakeholders have commented about the re-KYC and physical verification that it may disproportionately impact genuine and legitimate users, and that such measures are not specifically mandated under existing license conditions, and that there shouldn't be additional KYC as periodic KYC is already undertaken in compliance with license conditions. The Authority notes that re-KYC under regulation 21A has been mandated with a view to ensure that the Sender suspected with high probability of making UCC must not have acquired telecom resources in violation of KYC norms, while physical verification has been mandated to ensure thorough KYC of enterprises suspected of causing UCC and to verify that the telecom resources are not misused by the Sender for sending UCC.

xvi. As far as mandate on reverification under existing license conditions is concerned, it is pertinent to refer to the instructions issued by the Department of Telecommunications, dated 07.12.2021 for reverification of existing mobile connections. The instruction *inter alia* includes the following:

- *Whenever a UCC complaint is received on DIU portal, the flagged mobile connection may be subjected to reverification. In case UCC complaint is received on TRAI portal (as per existing practice), the extant instructions as per TCCCPR-2018 regulations will be followed. (para 10).*
- *In case of UCC complaints, the reverification of reported mobile connection and its associated mobile connections (if required) shall also be conducted. (para 5, sub-para (iv), item (c).*

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

- *In case Licensee suo-motto identifies an existing subscriber as a non- bonafide user, reverification of such subscriber may be undertaken and mobile connection shall be disconnected in case of failed reverification. (para 5, sub-para (iii).*

A perusal of these instructions shows that several measures for reverification have been mandated by the licensor, which also include action to be taken by the Access Providers in accordance with the provisions of TCCCPR 2018 in case of UCC.

xvii. Regarding suggestion of one of the TSPs that action in cases of failed re-KYC should be differentiated from cases where Senders are found to be misusing telecom resources for UCC activities, it may be seen that in case of failed KYC, the regulation provides for action as per extant KYC norms while in case of misuse of resources for sending UCC, the regulation 21A itself provide for enforcement action. Further, on suggestion for no additional KYC requirement for enterprise customers who undergo periodic KYC, it is noted that periodic KYC mandated for the enterprise customers is a licensing requirement while the reverification to be undertaken in case of AI-based detection of spamming activity is a regulatory mandate to undertake reverification as soon as the threshold criteria is met for the suspected Sender so as to prevent further UCC.

xviii. On the issue raised by some stakeholders about the privacy and security while KYC identifiers are shared among the operators, the Authority notes that the Access Providers are licensed entities, and for taking action against the Senders in case of fraud or UCC, they already share, as part of legal/ regulatory obligations, the KYC identifiers among themselves with minimum details required to identify the Sender and telecom resources associated with the Sender.

xix. Regarding the suggestion of one stakeholder to test the AI/ML-based systems with the banking industry, the Authority observes that the Direction for institutionalisation of AI/ML-based intelligence for inter-operator sharing and investigation of the suspect Senders has already been issued on 27.02.2026 and now its provisions have been incorporated as the regulation 21A. As already noted above, it does not provide for any enforcement action solely on the basis of AI-based intelligence.

xx. There was another suggestion from one stakeholder for use of volume-based triggers prior to complaint-based triggers in AI-driven flagging systems. Regulation 21A mandates a criterion of 'five or more CLIs of the Sender getting identified as "Suspected high probability UCC CLI" within the last ten days' for initiating further investigations while amendment to regulation 25 provides for lowering of threshold for triggering action against UTMs from 'five' to 'three or more complaints from unique recipients in last 10 days' provided any CLI allotted to the Sender has been identified or maintained as "Suspected *high probability* UCC CLI" by the AI system during the same period. In defining these criteria, the Authority has adopted a considered approach by tweaking the existing criterion for action under regulation 25. However, considering the diverse and dynamic nature of the ecosystem, the Authority, as per sub-regulation 25A(i), may classify Senders into different categories, and specify differentiated criteria for initiation of action and differentiated sets of enforcement measures applicable to such categories of Senders from time to time. Accordingly, based on the outcomes from the working of these regulations, a differentiated approach may be adopted from time to time.

xxi. The Authority further notes that the suggestion by a stakeholder for sharing the promotional complaints with Senders for response or investigation only after analysis of call recordings, cannot be accepted as recording calls involve several technical, legal and privacy issues and, therefore, cannot be mandated in routine. Moreover, such an onerous condition cannot be placed on recipients who are already facing the menace of UCC. Similarly, as the flagging is done on the basis of behavioural analytics and does not constitute conclusive evidence, throttling or blocking of spammers immediately after flagging has not been provided for in the regulations.

9. Misuse of Headers and/or Content Templates:

A. Stakeholders' Comments:

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

a) One stakeholder suggested to add "OAP to inform the suspension activity to the Header/Content template registrar TSP and registrar TSP shall issue a notice to the Sender".
b) Another stakeholder suggested to mandate multi-factor authentication for portal/API access, API key rotation, signed API requests, and delivery entity chain logs for CPaaS/aggregators, to support future enterprise automation.
c) Another stakeholder requested to review the timeline for issuing of notice and suggested to revise it to 24–48 hours.
d) A stakeholder suggested that the Authority may clarify what action is to be taken by the TSP if the action by the Sender is not taken as per the timelines of the regulation.
e) In case of filing complaint with LEA, one stakeholder suggested that in case of "PSU/Private/Govt" enterprises, the decision would be taken by respective OAP on case-to-case basis considering such steps should not lead to disruption of genuine messages to consumers.
f) Another stakeholder requested removal of the sub-regulation 22(1)(a) (ii)-3 regarding deregistering all such misused headers and content Templates since the PE is revoking the access credentials, there would be no need for de registering all headers and content templates.

B. Analysis and Conclusion:

i. The Authority considered it necessary to firstly define what constitutes 'misuse' under sub-regulation (1)(a) of regulation 22. Accordingly, the same has been defined in the form of an explanation.
ii. Regarding misuse of SMS headers and/or content templates, the regulations mandate 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.
iii. However, suspending all the traffic from Senders, especially, entities like government bodies, banks etc. may result in large scale disruption of services, hence, only the misused header and content templates may be suspended initially. However, if the Sender in whose name the headers and content templates have been registered, does not take corrective action in a reasonable time, all the traffic may be suspended from the Sender until such corrective action is taken by the Sender.
iv. Therefore, the amendment provides for suspending misused headers and content templates by the OAP within 6 hours of coming into its notice such misuse, and the OAP shall issue a notice to the Sender within 48 hours of the receipt of such information. As far as issue of notice in this regard to the Sender is concerned, one of the stakeholders has mentioned that only the registrar Access Provider would be able to issue notice to the Sender since the contact details of the Sender are available with registrar Access Provider only. However, during consultations, it was clarified by the Access Providers that the contact details of the Sender are available on the DLT platform and, therefore, notice to the Sender can be issued by the OAP. In case Sender fails to take corrective action, all the commercial communication traffic may be suspended from the Sender until corrective action is taken by the Sender. It is further noted that based on the suggestions of the stakeholder to revise timelines for various actions under the regulation, suitable modifications have been done keeping in view the practical aspects.
v. The Authority has also observed that there have been cases where misuse was either done by the Telemarketer, or the Telemarketer was an accomplice in the misuse. Though the extant regulation provide for filing complaint by the Sender against such Telemarketer with the law enforcement agencies under relevant laws, it is felt that there is also a need to provide for regulatory action against the Telemarketers in such cases. Accordingly, it has been 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. Moreover, the OAP and all the other Access Providers must take action against such Telemarketer as provided for in the amended regulation. It is pertinent to note that keeping in view the severe consequences of misuse, the amendment provides for disconnecting all the telecom resources of such Telemarketer across all the Access

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

Providers for a period of one year along with blacklisting during this period. The Authority notes that this action shall be without prejudice to any action that law enforcement agencies may take against such Telemarketer.

vi. Further, in case the misuse has occurred due to leakage, cloning, or compromise of credentials, the regulation also mandates the de-registration of all the Headers and Content Templates of the Sender to prevent their misuse. One of the stakeholder has suggested to remove this sub-regulation on the basis that once the Sender has revoked the access credentials, there would be no need for de registering all headers and content templates. The Authority notes that this is not a correct and complete appreciation of the process. While registration is done by a Sender using the credentials at the Access Provider's portal, the traffic is sent using the portal provided by the Telemarketer/ aggregator. Once the PE Id, Header ID and Content Template Ids are leaked, the entity in possession of such details may send messages using these details at TM's portal, misusing such unauthorizedly acquired credentials of the genuine Sender provided by the Access Provider. Accordingly, it is necessary that all the Headers and Content Templates of the genuine Sender are de-registered and new Ids are issued against them through re-registration.

vii. However, the Authority observes that there may be cases where immediate bulk de-registration may materially disrupt essential commercial communications or cause significant inconvenience to the consumers. This concern has been raised by a few stakeholders also. Accordingly, it has been provided that in such cases, the de-registration may be done in a phased manner.

viii. Regarding the comment of a stakeholder to adopt various security measures such as multi factor authentication etc, the Authority notes that two factor authentication is already implemented. Further, multifactor authentication needs to be weighed against the complexity and compliance burden, especially, for smaller PEs. Hence, this can be considered in future on need basis.

10. Accountability of Senders and TMs: Amendment to Regulation 22

Stakeholders' Comments:

a) Some of the stakeholders commented that Telemarketers (TMs), Aggregators, and Principal Entities (PEs)—as key stakeholders in the communication ecosystem—should be explicitly brought under the regulatory framework by TRAI, with clearly defined roles, responsibilities, and accountability mechanisms.

Analysis and Conclusion:

i. The Authority notes that regulation 22 includes various provisions for ensuring accountability of the Senders and TMs such as provisions for charging fee for registration and taking security deposit by the Access Providers from the Senders/ TMs, imposing FDs on them for non-compliance etc. Moreover, the proviso to sub-regulation (1)(f) enables the Authority to specify the fee for registration or it may direct the Access Providers to specify such fee while the proviso to sub-regulation (1)(g) enables the Authority to direct the Access Providers to take appropriate measures in case measures specified by the Access Providers against the registered Senders and Telemarketers are not effective. Besides, the sub-regulation (1)(i) also mentions some of the key aspects which have to be taken care of by the Access Providers through agreements with the Senders/TMs to ensure compliance with the regulatory framework.

ii. However, it has emerged during consultation with the Access Providers that in absence of uniform provisions that might have been mandated as essential conditions of the agreement between the Access Providers and the Senders/TMs, the Access Providers are not incorporating such terms and conditions in the agreement primarily due to commercial interest as stricter conditions imposed by an Access Provider may lead to migration of the Sender/TM to another Access Provider with relaxed conditions. In view of this, the Authority is of considered view that there is a need to have an enabling provision in the regulations whereby the Authority may specify the essential conditions of the agreement between the Access Provider and the Sender or the Telemarketer, which have to be mandatorily made part of such agreement, for preventing the misuse of telecom resources for sending UCC by the Sender or the Telemarketer. Accordingly, the amendment has included a proviso to this effect to the sub-regulation 22(1)(i).

11. Appeal Mechanism

A. Stakeholders' Comments:

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

a) One of the stakeholders commented that a reasoned order provided as part of complaint resolution strengthens transparency and auditability.
b) It was suggested to provide online unified portal/ app for complaints and appeals.
c) Some of the stakeholders commented that an appellate framework already exists for all complaints within the Telecom Consumer Complaint Redressal Regulation (TCCRR) ecosystem, which is adequately equipped to handle consumer grievances. A separate redressal mechanism for only UCC complaints will create a duplication. It would impose significant administrative burden on TSPs, restructuring of internal processes, and ongoing compliance costs, which may not be as per intended outcomes. It was informed by one of the TSPs that the appeal is presently taken by the TAP on CRM and it does not flow on DLT nor to any other TSPs. Building this flow needs entire system development on DLT for both TAP & OAP, and will incur huge costs and efforts.
d) One of the stakeholders commented that while conceptually correct, the technical feasibility and ecosystem readiness must be re-evaluated. Concerns are raised regarding practical feasibility, especially due to the absence of a robust, tech-enabled system on the DLT platform for appeals, and, hence, reconsideration is suggested.
e) On the other hand, one of the stakeholders suggested to have the complete appeals' workflow recorded on the DLT platform as it would improve transparency for complainants, enable regulatory audit of compliance with appeal timelines, and support greater consistency in decision-making across Access Providers. It would also create a useful body of recorded outcomes that may inform future enforcement practice.
f) One stakeholder commented that there would be no change in the outcome of the original resolution even in case of an appeal. In both the cases the resolution of the complaint will rely on the same system records and CDRs. It will increase the burden of compliance and the operational costs, in contrast to the principle of Ease of Doing Business.

B. Analysis and Conclusion:

i. A number of representations are received by the Authority from customers who are dissatisfied with the manner in which their complaints have been resolved by the Telecom Service Providers (TSPs) wherein complaints are often closed citing inadequate or incorrect reasons. The performance monitoring reports (PMRs) received from the Access Providers for the period from January'26 to June'26 show that out of 2,07,500 UCC complaints received against the registered Telemarketers (RTMs) during this period, the Access Providers closed 1,65,828 complaints as invalid complaints which is about 80% of total RTM complaints during this period. Similarly, for the same period, out of 16,40,309 UCC complaints received against the unregistered Telemarketers (UTMs), the Access Providers closed 5,11,792 complaints as invalid complaints which is about 31% of total UTM complaints received during this period. Such a situation creates dissatisfaction among the customers. Further, it has also been observed that the responses communicated to customers are often vague, unclear, and ambiguous. Hence it becomes important to have an appeal mechanism which is effective.

ii. The Authority notes that the appeal mechanisms presently provided by Access Providers for UCC complaints are limited to modes such as call centres, e-mail, post, or in-person submissions. In order to strengthen the regulatory framework, it is imperative that all the modes of UCC complaint lodging made available to customers under TCCCPR 2018 are also enabled for preferring appeals before the Appellate Authority of the TSP. Such a suggestion has also been received from few stakeholders. Moreover, it is necessary that the appeal process needs to be efficient and customer-centric, and the appeals need to be addressed effectively in a fair, transparent and time bound manner.

iii. The Authority notes that an appellate framework for the complaints already exists under the Telecom Consumer Complaint Redressal Regulations (TCCRR), and therefore, a separate appellate framework may not be required for appeals in case of UCC complaints. Considering the same, the regulation has been amended to mandate that the Appellate Authority shall resolve and reply to such appeals in a manner and within a period as prescribed under TCCR Regulations.

iv. It was informed by one of the TSPs that the appeal is presently taken by the TAP on CRM and it does not flow on DLT to any other TSPs. Building this flow needs entire system development on DLT for both TAP & OAP,

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

and will incur huge costs and efforts. The Authority observes that appeal has to be addressed by TAP or OAP depending upon which Access Provider has closed the complaint as per the obligations assigned to them under Complaint Mechanism vide Regulation 25, and, therefore, has to flow through DLT platform. Accordingly, it has been mandated that the Access Providers shall establish the necessary mechanism for communicating the appeal received by the TAP to the concerned Appellate Authority at OAP. This shall also include the appeals received by the TAP through any of the modes specified under TCCRR, 2012 i.e. through email, mobile application, website/portal, complaint centre, or post or in person.

v. Regarding the comment that there would be no change in the outcome of the original resolution even in case of an appeal as in both the cases, the resolution of the complaint will rely on the same system records and CDRs, the Authority does not agree to this comment. While auditing the complaint closure done by the Access Providers, the Authority has observed that a significant number of complaints are closed improperly by the Access Providers as already mentioned at para (i) above. Often, the service providers entrust complaint handling to outsourced agencies, CHAT bots, AI agents, etc., which many times do not resolve grievances satisfactorily. Accordingly, there is an indispensable need to have an appeal mechanism at appropriate level.

vi. In proviso (a) of sub-regulation (5) which deals with the minimum requirement for a complaint to be valid, it has been noted that for Sender as well as complainant, the phone number has been mentioned as 'mobile number'. However, the number can be a fixed line number also. Accordingly, 'mobile number' has been replaced with 'telephone number'.

12. Retention period of complaint and appeal records: Amendments to Regulation 24

A. Stakeholders' Comments:

a) Many stakeholders suggested that record period should be only one year. They submitted that existing platforms of DLT and CRM systems are not designed to store such large volumes of data over extended periods. Further, Compliance with this requirement would necessitate considerable augmentation of storage infrastructure, leading to increased cost, and system complexity.

b) One of the stakeholders supported 3-year records and suggested to add privacy safeguards and consumer access rights:

c) It was also suggested to extend record retention to include model/automation decision metadata such as decision rule category, timestamps, evidence pointers etc to enable future auditability of AI enforcement.

B. Analysis and Conclusion:

i. Sub-regulation 3 of regulation 25 provides in case a complaint is reported by any customer after seven days of receipt of UCC by the customer, it is closed by the Terminating Access Provider and its status is changed as "report" instead of "complaint". Such reports, although not treated as complaint yet they provide useful information about the behavioural pattern of the Sender, and also prove useful as evidence while investigating complaints against the Senders. However, it has come to the notice of TRAI that reports are not being recorded by Service providers. Therefore, it has been mandated that every complaint, appeal or report of the unsolicited commercial communication by the customers, shall be recorded by the Terminating Access Provider as well as the Originating Access Providers.

ii. The requirement to maintain complainant-wise records of complaints, appeals and reports along with supporting documents, has been added to facilitate examination of disposal of complaints and appeals. The absence of such records has been creating difficulties in assessing and verifying whether complaints and appeals are being disposed of in accordance with the provisions of the Regulations.

iii. As far as period of retention of such data is concerned, the Authority observes that the Unified Licence (UL) Agreement pursuant to the amendment dated 21.12.2021, mandates retention of commercial records/ Call Detail Record (CDR)/ Exchange Detail Record (EDR)/ IP Detail Record (IPDR) data for two years. Rule 45(2) of the Telecommunications (Authorisation for Provision of Principal Telecommunication Services)

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

Rules, 2026, similarly mandates maintaining all commercial records, subscriber data record, call data record or call detail record, exchange detail record, internet protocol detail record or internet protocol data record and any other similar records for a period of two years.

iv. Considering the comments of stakeholders to reduce the retention period of record, the Authority has aligned the retention period with that provided under the Unified Licence (UL) Agreement/ Telecommunications (Authorisation for Provision of Principal Telecommunication Services) Rules, 2026, and has mandated to maintain complaints record including appeals, and reports for a period of 2 years.

13. Complaint Mechanism, Sender classification and Differential Regulatory Action

A. Stakeholders' Comments:

a) It was commented by a stakeholder that the term "Sender" should refer only to the Principal Entity and not Telemarketers, since Telemarketers merely act as technical intermediaries between Access Providers and Principal Entities, and neither control the content nor derive commercial benefit from the communication.

b) One stakeholder suggested to provide a 24–48 hour "consumer correction window" before closure of incomplete complaints. It was also suggested by a stakeholder to extend the complaint admissibility window from 7 days to 15 days and treating complaints filed within this period as valid "complaints" rather than mere "reports". However, some of the stakeholders opposed extending the complaint registration timeline beyond 7 days, citing operational challenges.

c) Another stakeholder suggested to include an appropriate provision for providing that the Terminating Access Provider should be the primary Authority for recipient-side compliance determination including aspects of scrubbing against preferences and consents, while the Originating Access Provider should remain responsible for all Sender-side examination and enforcement including examination of Sender KYC, header and template correctness, and action against the telecom resources allotted by it. In case of delivery of any promotional content through transactional or service route, the responsibility should rest with the Originating Access Provider.

d) One stakeholder suggested to introduce structured proportionality factors such as severity, number of consumers affected, repetition, and mitigation steps before imposing stringent enforcement actions like network-wide disconnection, to ensure fairness and avoid large-scale disruption.

e) A stakeholder suggested to provide at least three business days to TAP to act after expiry of the Sender's representation period, allowing Senders an opportunity to submit justification or consent proofs. It was also submitted by the TSP that barring outgoing services on PRI/SIP links is not technically feasible and remains an industry-wide challenge. Another stakeholder proposed to increase the investigation timeline for complaints relating to misuse of numbering series to at least three business days, citing that one-business-day window is inadequate.

f) Some of the stakeholders suggested that the enterprises should be considered as a distinct Sender category with differentiated thresholds, contextual evaluation criteria, customised complaint-handling processes, and a graded enforcement mechanism. It was also suggested to increase the complaint threshold for enterprise Senders to 50 complaints within 7 working days to avoid disproportionate enforcement actions against high-volume legitimate communications. One of the stakeholders suggested the threshold of 50 complaints in last 15 days, a minimum seven-business-day notice period, and a graded four-step enforcement mechanism ranging from warning to blacklisting.

g) It was also suggested to restrict penal action only to the specific offending telecom resources instead of blocking all resources of an entity, and sought differentiated enforcement treatment for Systemically Important Banks (SIBs), noting that blanket blocking could disrupt critical banking services such as OTPs and transaction alerts.

h) One TSP commented that the telecom resources issued for purposes other than the alleged violations, such as 140/1600/1800 numbers, M2M SIMs, leased lines, and broadband, should not be disconnected, and that barring and tracking of all devices would be highly cumbersome and unimplementable.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

i) One stakeholder commented to replace immediate suspension provisions with an urgent show-cause notice and a 48-hour cure period, after which suspension should occur only if the Sender fails to respond or the investigation confirms a violation, to avoid disruption arising from false positives or legitimate high-volume communications.

B. Analysis and Conclusion

i. For the purpose of regulation 25, the regulation specifically mentions that Sender includes Telemarketer, and accordingly, action against the telecom resources of the Sender or Telemarketer used for sending UCC, as the case may be, will also be taken in case of non-compliance. While the SMS sent by the RTMs using SMS headers and content templates are on behalf of Senders, and promotional calls made using 140 series numbers are scrubbed at preference registry, in case of UTMs, no differentiation can be made between a Sender and a TM.

ii. Regarding comment about incomplete complaints, the Authority notes that sub-regulation 23 (5) already mandates the Access Providers to provide details of format and procedure to the customer in case of incomplete complaints. Using this information, a customer can file the complaint in proper format. On the suggestion of a stakeholder to extend the complaint admissibility window from 7 days to 15 days, the Authority is of the opinion that 7-days period is adequate since a complaint contributes to the evaluation of the threshold of '5 or more complaints in last 10 days' over a period of next 9 days from the date of complained communication. Extending complaint admissibility window beyond 7 days would unduly prolong the regulatory action cycle besides increasing the data management requirement. Moreover, extending the window beyond 7-days can also result in wrong complaints since customers may not be able to recall necessary details of the communication that took place long back. Further, a subscriber aggrieved by UCC is likely to complain at the earliest rather than complaining for an event that occurred more than 7 days ago.

iii. It has been commented by a stakeholder that the Terminating Access Provider should be responsible for recipient-side compliance determination including aspects of scrubbing against preferences and consents, while the Originating Access Provider should remain responsible for all Sender-side examination and enforcement. The Authority notes that the regulatory provisions already take care of these aspects. Besides, as far as aspect such as scrubbing against preferences and consents is concerned, the regulations prescribes the obligations of Access Providers, and based on the technical requirements, the responsibility may be assigned to OAP or TAP as appropriate.

iv. As far as introduction of proportionality factors before imposing stringent enforcement actions is concerned, the Authority notes that the regulation already provides for alerting the Sender through notification whenever any complaint against the Sender is received. Also, the regulation provides for graded action against the Senders engaged in sending UCC. Besides, these amendments include enabling provisions for the Authority to classify the Senders into different categories, and specify differentiated criteria for initiation of action and differentiated sets of enforcement measures for such categories.

v. Regarding the suggestion of a few stakeholders to increase the investigation timeline to at least three business days, it may be seen that regulation 25 already provides for carrying out investigation and taking action by the OAP within five business days from the date of receipt of representation from the Sender or expiry of the five business days' notice period given to Sender for representing the case.

vi. On the comments of a stakeholder that barring outgoing services on PRI/SIP links is not technically feasible, the Authority notes that under the regulations, the action has to be taken against all the telecom resources of the UCC Sender across all the TSPs. Hence, in case of non-compliance, whole PRI/SIP links need to be barred, and not individual DID numbers.

vii. Another issue raised by some stakeholders is that the enterprises employing large number of telecom resources including SIP/PRIs/numbering resources (MSISDNs) etc. for commercial communications, should be considered as a distinct Sender category with differentiated set of actions. The Authority observes that on one hand, the enterprises have more potential to send UCC, while on the other, there are also more chances of error by their agents in sending the commercial communications to the recipients against the preferences and consents of the recipients. Further, while action against the Senders for sending UCC include barring outgoing services

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

of all their telecom resources for 15 days for first violation, and disconnection of all their telecom resources for one year and blacklisting for subsequent violations, such action in case of entities such as banks, can cause large scale disruption of their services, thereby, having large adverse impact for the consumers and sometimes economy as a whole. Therefore, a different action for violation may need to be prescribed. However, considering that the commercial communication eco-system is a multistakeholder system, having not only different type of entities such as Principal Entities (Senders) and Telemarketers with different scales of operation but also that these are also from different sectors. Therefore, the Authority is of the view that a "one-size-fits-all" approach may not work for all types of enterprises. Accordingly, the amendment introduces a regulatory provision through sub-regulation (i) of newly inserted regulation 25A whereby Senders may be classified based on criteria such the importance of the entity to the economy or to a critical sector, the criticality of services being delivered to consumers, the nature and regulatory status of the entity, the scale and volume of operations, the extent and manner of usage of telecom resources, the potential impact of suspension/ disconnection of telecom resources on consumers etc.; and to specify different set of actions to be taken against different classes of Senders for violations from time to time. It is noted that the published draft regulation has proposed such provision under different regulations at various places. However, for more clarity and to avoid repetition, the provision has been removed from multiple places and provided as a sub-regulation under regulation 25A.

viii. It is further noted that the clause (f) of sub-regulation 4 prescribes the regulatory action to be taken in case of misuse of the number resource(s) allotted from series assigned for transactional and service calls, for making promotional Voice Calls. Presently, 1600 series has been designated for transactional and service calls by entities in BFSI sector and 1601 series has been designated for such calls from Utilities, Logistics and Courier companies. The extant clause (f) of sub-regulation 4 provides for stringent action for misuse of such series that includes suspension, outgoing barring or disconnection of all the telecom resources of the Sender across all Access Providers and also blacklisting. However, considering the critical role that entities in BFSI sector entities have, it may not be desirable to take such action against the entities such as banks, insurance companies etc that use 1600 series as this may adversely affect the consumers as well as various commercial operations critical to the economy. Similarly, calls from any other series designated by the Authority for service and transaction calls are going to be important for the customers. For examples, the Authority has recently permitted use of 1601 series numbers for the entities such as utilities, logistics and delivery. Therefore, the Authority is of the view that while there is a need for effective action against misuse of these special series, such action should take into consideration factors like criticality of services being delivered to consumers. Moreover, considering the dynamics of the ecosystem, the graded actions against misuse need to be updated from time to time based on evolving situations of extant of misuse and the impact of regulatory action in terms of corrective action as well as on continuity of critical services. Accordingly, it has been provided that in case of complaints against numbers from series designated for service and transactional calls, the action shall be taken by the Access Provider as directed by the Authority from time to time.

ix. Regarding the suggestion of restricting the action only to the specific offending telecom resources instead of blocking all resources of an entity, the Authority is of the view that such an approach is unlikely to help as UCC Senders normally make use of many telecom resources for sending UCC. As the action under the regulation is based on complaints, if action is restricted only to specific offending telecom resources against which the complaints have been received, they can easily switch telecom resources or acquire new telecom resources from other Access Providers for sending UCC. Accordingly, the deterrent would be effective only if action is taken against all the telecom resources of the Sender across all the Access Providers. It is also observed that considering the ability of UCC Sender to use and switch multiple telecom resources across various Access Providers, the regulatory framework envisages that the threshold of number of complaints as well as AI-based flagging is to be checked by the OAP across all the Access Providers.

x. To strengthen the regulatory framework, the Authority is of the view that the details of blacklisted entities also need to be published in such form, manner and at such time as the Authority considers appropriate. Besides

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

acting as a deterrent, it would also inform the public in general about such entities as well as strengthen their trust in the effectiveness of the regulatory framework.

xi. On the comment of a stakeholder to replace immediate suspension provisions with an urgent show-cause notice and a 48-hour cure period, it has already been noted above that the Sender is notified about each complaint so as to enable the Sender to take timely corrective action. Suspension of the telecom resource used for sending UCC is done by the OAP only when complaint threshold is met, and, thereafter, the Sender is given a reasonable opportunity to represent before graded action is taken. Therefore, the Authority is of the view that existing provisions in this regard are in order.

xii. It has also been noted that there exists multiple provision in the regulation whereby Authority may specify various operational aspects of implementations from time to time, which makes the regulation look complex. This includes items such as prescribing the format, content and manner of sending notifications to customers and Senders; manner and format for publishing the information etc. Therefore, to simplify and make the regulations lighter, these scattered provisions have been deleted and sub-regulation (ii) under regulation 25A has been introduced whereby to ensure effectiveness or consistency of the implementations mandated under the Regulations, the Authority may prescribe various operational implementations as required from time to time.

14. CDRs for Audit, and Maintaining record of alleged violations

A. Stakeholders' Comments:

a) Many stakeholders 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.

b) It was also suggested by a stakeholder to remove the clause. It was submitted that the CDRs can be provided only to security agencies designated by Department of Telecommunications under the Telecommunication Act 2023 and corresponding rules.

c) On the other hand, one stakeholder suggested to keep the period of CDRs sought as maximum one hour around the event.

d) One of the stakeholders suggested to add safeguards such as limiting CDR provision for limited periods, purpose-limited to audit/investigation, with confidentiality and security controls.

e) It was also commented by a stakeholder that the CDR audit mechanism is necessary in light of the data showing 11.4% of complaints closed on "CDR mismatch" grounds during August–November 2025.

f) It was suggested to expand sub-regulation (4A) to explicitly cover AI flagging audit and false-positive examination, not only complaint closure.

B. Analysis and Conclusion:

i. During the analysis of UCC complaints for the period Aug-2025 to Nov- 2025, it was noted that 11.4% of complaints were closed on "CDR mismatch" grounds. Similarly, for the period Jan-2026 to April- 2026, it has been observed that total 12,37,707 complains were lodged by the customers, out of which 3,66,900 complaints were closed as "invalid complaints" which included 1,32,137 complaints i.e.10.68%, declared invalid on the ground that CDR did not match. Considering that a significant number of complaints are being closed on the ground of 'CDR not matching', there is a need to check the correctness of such closures by auditing the details of such CDRs. Accordingly, Authority has decided that there should be no change regarding the amended provision for providing CDRs by OAPs and TAPs as requested by TRAI. However, CDRs sought will only be for the period relevant for analysing the complaint closures, as suggested by many stakeholders.

ii. The provision on AI flagging and its scope is already discussed elsewhere in the explanatory memorandum.

iii. Sub-regulation 3 of regulation 25 provides that in case a complaint is reported by any customer after seven days of receipt of UCC by the customer, it is closed by the Terminating Access Provider, and its status is changed as "report" instead of "complaint". Such reports, although not treated as complaint yet they provide useful

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

information about the behavioural pattern of the Sender which can be used for UCC detection under Schedule-IV, and also prove useful as evidence while investigating complaints against the Senders. However, it has come to the notice of TRAI that reports are not being recorded by Service providers. Accordingly, the amendments provide that record of every alleged violation of the regulations reported by the customers of Access Provider as well as reports of alleged violations of the regulations received from the other Terminating Access Providers shall be recorded by the Access Provider. Moreover, sub-regulation 3 of regulation 24 provides for maintaining the records of complaints, appeals and reports for two years.

iv. Regarding the comment of a stakeholder to expand sub-regulation (4A) to explicitly cover AI flagging audit and false-positive examination, the Authority notes that audit of AI flagging has not been envisaged as of now, and has to be governed by the Access Providers as per their AI Governance Policy. In this regard, Analysis on Regulation 21A above may be referred where it has been mentioned that AI-generated intelligence does not, by itself, constitute conclusive evidence for enforcement action as the possibility of false positives cannot be entirely ruled out. Therefore, the regulation does not provide for treating AI-based flagging as a self-sufficient an independent basis for punitive regulatory action. The AI-based flagging only acts as a trigger for further investigation into the cases of suspected UCC, and regulatory action is only initiated based on the findings of the investigations. As far as false positives are concerned, Regulation 21A also mandates the Access Providers to provide a mechanism to the Senders whose CLIs have been flagged as "Suspected UCC/spam" to represent their case with justification against the flagging, and shall unflag the CLIs if justification is found in order.

15. Amendments to Regulation 27

i. The Authority has observed that in case of imposition of financial disincentives, the heading of the Regulation 27 viz. "Consequences for failure to curb the Unsolicited Commercial Communications from registered Senders or RTMs" has often been misinterpreted by the Access Providers to defend the non-compliance. It is argued by them that the Access Providers do not have any control over the Senders and Telemarketers. The Authority notes that FD is imposed on the Access Providers not because of the reason that Senders/ Telemarketers against whom complaints have been received, have sent UCC but because of the failure of the Access Providers to take action against the telecom resources of the UCC Senders/ TMs in accordance with the Regulations. Appropriate resolution of UCC complaints, based on which action on the telecom resources of UCC Senders/ Telemarketers can be taken, is the key to controlling UCC, and failure to perform these obligations let such Senders/ Telemarketers to continue sending UCC unhindered. It is observed that the Regulations do not impose any functions or obligations on Access Providers that lie beyond their control. The financial disincentives are imposed for non-performance of the functions that are wholly within the control of the Access Providers. Accordingly, to bring more clarity, the words "Consequences for failure to curb the Unsolicited Commercial Communications from registered Senders or RTMs" in the heading of the Regulation 27 have been substituted with the words "*Consequences of failure to take action against registered Senders or RTMs for sending Unsolicited Commercial Communications*".

ii. Regarding the imposition of the financial disincentive under existing item (a) of sub-regulation 27 (1), the OAP is liable to pay as financial disincentive, an amount of one thousand rupees per count of valid complaint that is declared invalid. This amended provision was introduced in February-2025, making FD applicable on valid complaints that is declared invalid by the Access Provider. Before, the amendment, the regulation provided for imposition of FD on all valid complaints against RTMs since UCC from RTMs could have bene stopped by the Access Providers through scrubbing carried out in relation to 140 series numbers, SMS Headers and Content Templates, and any valid complaint against UCC from RTMs would originate due to failure of the Access Providers to do proper scrubbing. However, the amendment was introduced as in some cases such as those related to misuse of 1600 series, the Access Provider cannot, through scrubbing, stop the communication from taking place. Such complaints are to be investigated by the Access Providers and in case the complaints are found valid, the action is to be taken against the Senders as per regulatory provisions. Therefore, in such cases, it would not be appropriate to impose FD on the Access Provider merely on the basis of existence of valid complaints. Accordingly, the aforesaid provision was amended to make FD applicable on valid complaints that

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

is declared invalid by the Access Provider. However, subsequent to the amendment of February-2025, a gap has been observed in regulatory provisions in relation to those valid complaints which originate due to the failure of the OAP to carry out proper scrubbing. Therefore, this amendment provides for imposing FD on the Access Provider on the basis of existence of valid complaints where such UCC from RTMs have originated due to failure of the OAP to carry out the scrubbing in accordance with the preference and consent of the customer. Accordingly, a proviso has been added to this effect in clause (a) of sub-regulation 27(1).

16. Wrong categorization of Content Templates, registered by an Access Provider other than the OAP

A. Stakeholders' Comments:

The stakeholders made the following comments and suggestions regarding the proposed draft amendment on the issue:

a) Many stakeholders agreed for fixing the accountability on registrar Access Provider but opposed the shared liability on OAPs. They recommended stricter enforcement against non-compliant or exploitative entities. It was commented that the introduction of shared liability between OAPs and registrar TSP in cases of wrong categorization increases the compliance burden as the OAP, as a transmission channel, has limited control over Sender behaviour, which creates a disproportionate liability. It was suggested that the financial disincentive be limited to registrar TSPs only.

b) It was proposed that the financial disincentives be limited to cases of incorrect registration or template categorization, along with a graded additional security deposit framework for repeated UCC violations by Principal Entities, namely: ₹1 lakh on the first complaint notice, ₹1.5 lakh on the second violation notice, and ₹4 lakh on the third violation notice, to be deposited by Second party, with forfeiture of previously deposited security amounts in case of continued violations, supported by PMR-based verification.

c) It was also commented that the liability for incorrect template categorisation should not rest solely on the Sender since the Access Provider also plays an approval role, and suggested providing a correction window (e.g., 3 business days).

d) Sender suspension for wrong template categorisation should apply only where five templates are blacklisted within a 90-day period and involve two or more distinct categorisation errors, to avoid disproportionate penalties arising from a single repeated classification mistake.

e) One of the stakeholders proposed that where 80% or more content templates of a Sender are blacklisted due to wrong category registration, then the entity should also be blacklisted.

f) One of the stakeholders suggested to delete *'and if five………'* and replace it with *'Registrar TSP to reverify all the content templates of the Sender for registration under proper category,'* noting that tracking blacklisted templates across DLT platform is operationally impractical under the current framework.

g) One stakeholder sought clarification on whether the threshold of five blacklisted templates applies cumulatively across all TSPs or individually at the OAP level. It was also submitted that the proviso warrants bifurcation into two distinct categories to address the underlying issues more precisely viz. (i) instances of misuse of templates by Telemarketers/Principal Entities through insertion of unsolicited or non-compliant content within the variable portion of approved templates; and (ii) cases of incorrect or non-compliant template registration attributable to Registrar TSPs; and proposed separate treatment for the two categories.

h) It has been suggested to strengthen deterrence against wrong category registration of content templates by retaining template blacklisting, mandating root-cause analysis and corrective controls for repeated mis categorization while permitting continuity of essential transactional communications for critical sectors while restricting promotional communications.

B. Analysis and Conclusion:

i. During auditing the complaint closures done by the Access Providers, the Authority has observed several cases where UCC originates because of the registration of content templates by the Senders under wrong category with the registering Access Provider e.g. a content template having promotional content but registered under

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

service category. TRAI has issued Direction dated 20.08.2024 regarding measures to curb misuse of Headers and Content Templates which, inter alia, mandates the blacklisting of such content templates by the OAP, and suspending the services of the Sender if five content templates of such Sender are blacklisted for registration under wrong category. Such suspension shall be for one month or till such time all the content templates of the Sender are reverified for registration under proper category, whichever is later. One of the stakeholders has suggested to suspend the services of the Sender only where five templates are blacklisted within a 90-day period, and involve two or more distinct categorisation errors. The Authority finds merit in the suggestion of the stakeholder for limiting the period to 90 days, within which blacklisting of five templates is to be checked by the Access Provider. However, the same may be reviewed by the Authority from time to time to ensure the effectiveness of the measure. Regarding the comment to take action only if two or more distinct categorisation errors are involved, the Authority is of the opinion that besides operationally challenging, such a condition would lead to significant dilution as most of the cases pertain to categorising promotional message as service message. Based on the above considerations, the proviso to item (d)(ii) of sub-regulation 25 (4) has been introduced.

ii. On the comment of a stakeholder that registrar TSP should reverify all the content templates of the Sender for registration under proper category, it is noted that the amendment already provides for the reverification of registration of all the content templates of the Sender under proper category, before the services of the Senders are restored Here, it is necessary to clarify that the threshold of five blacklisted templates applies cumulatively across all the Access Providers as the regulatory framework envisages action against non-compliant Senders across all Access Providers to make it effective. Otherwise, the UCC Senders may keep on changing their Access Providers and acquiring new telecom resources for sending UCC which will defeat the purpose of controlling UCC.

iii. As far as comment of one stakeholder to bifurcate the provision in two categories viz. (i) misuse of headers and content templates, and (ii) wrong categorisation of content templates, is concerned, the Authority notes that these are already dealt with under different provision – the misuse of headers and content templates is dealt with under item (a) of sub-regulation 22(1) while provisions related to wrong categorisation of content templates are contained in regulation 25 and 27.

iv. The draft regulations also contained certain provisions regarding primary registration and secondary validation of the content templates, and also those related to imposition of financial disincentives on registrar and Originating Access Providers in case of non-compliance. However, many stakeholders have opposed the draft amendment, suggesting to fix the accountability on registrar Access Provider but opposed the shared liability on OAPs, and have recommended stricter enforcement against non-compliant or exploitative entities. It was commented that the introduction of such shared liability increases the compliance burden as the OAP, as a transmission channel, has limited control over Sender behaviour, which creates a disproportionate liability. It was also argued that registrar Access Provider is under regulatory obligation to exercise due diligence while approving the content template and its categorisation. In this regard, the Authority took note of the proviso to item (a) of the sub-regulation 27(1) which was introduced as part of the amendments done in February'2025. It provides that where UCC has originated due to Headers and Content Templates registered by another Access Provider in violation of the regulations, and OAP has taken action against such UCC as per regulation 25, the financial disincentive as above shall be imposed on the Access Provider that has registered such Headers and Content Templates, instead of OAP.

v. The Authority notes that although the regulatory provision for fixing the responsibility of the registrar Access Provider already exists, the draft amendment was proposed considering that large number of unsolicited commercial messages get delivered when the Sender uses the service of some other Access Provider (OAP) to send such wrongly categorised messages, and, accordingly, it was proposed that OAPs may also have a preventive role through secondary validation of the content templates before sending the traffic. However, in view of the fact that the aforesaid proviso for fixing the responsibility of the registrar Access Provider has been

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

introduced in February' 2025, and, that it may be appropriate to observe its effects on the regulatory compliance for some more time, the Authority decides not to go ahead with the proposed amendment for the time being.

17. Restoration of Telecom Resources: Amendments to Regulation 29

A. Stakeholders' Comments:

a) All the stakeholders who commented supported the provision to introduce floor charges for restoration.

b) Most stakeholders submitted that restoration should be linked to verifiable remediation, and should follow a clearly defined, time-bound process with a structured workflow and specified timelines.

c) Another stakeholder submitted that restoration of telecom resources such as SIP connections, DID numbers, and ported-out resources may not always be technically or operationally feasible once they have been deactivated, reconfigured, or migrated to another Access Provider.

d) It was also submitted that numbering resources are governed by lifecycle management and recycling practices, due to which restoration may not be technically feasible in all cases.

B. Analysis and Conclusion:

i. Regulation 29 provides for the representation before TRAI by the Sender against whom action has been taken by the Access Providers, for restoration of telecom resources. It has been observed that some Senders approach TRAI for restoration of a smaller number of telecom resources and removal of blacklisting. The regulation provides for restoration charges of five thousand rupees per resource subject to maximum five lakh rupees. These restoration charges are intended as a deterrent for the Sender. Therefore, while a Sender requests for restoration of only few of its telecom resources, it needs to be ensured that the restoration charges should not become so low that they fail to act as a deterrent, and Senders start taking unfair advantage of the partial restoration process. Accordingly, considering the need for having a balance between these two aspects, it has been decided while a Sender may apply for restoration of only some of its disconnected resources, the minimum restoration charges should not be less than half of the restoration charges calculated to restore all the telecom resources of the Sender. Setting a minimum charge will discourage Senders from repeatedly violating rules.

ii. Further as many stakeholder submitted that restoration of telecom resources such as SIP connections, DID numbers, and ported-out resources may not always be technically or operationally feasible once they have been deactivated, reconfigured, or migrated to another Access Provider, the Authority has decided that restoration of such numbering resources may be done by the Access Providers subject to feasibility.

iii. The Authority also took note of the provision under sub-regulation (1) that allows for representation by the Sender before TRAI within sixty days of action taken against the Sender by the Access Provider. However, it is felt that there should be a provision for the Authority to allow such representation even after 60 days if the circumstances so warrant. Such representation may be entertained by the Authority duly recording the reason for considering the same. Accordingly, a proviso has been provided to this effect under regulation 29.

18. Amendments to Regulation 34A

A. Stakeholders' Comments on sub-regulation 34A (1)

The stakeholders commented as below:

a) That the regulation extends telecom regulatory obligations to OTT platforms and CMAs, encroaching upon domains governed by the Information Technology Act and MeitY, leading to regulatory overlap and a colourable exercise of delegated power.

b) That the provisions relating to call management applications should be addressed under a separate and clearly defined regulatory framework to avoid ambiguity and enforcement challenges. Clarity is also required on the legal basis, including applicability under the IT Act, to ensure effective enforcement.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

c) One of the stakeholders has commented to extend the applicability of relevant provisions of the TCCCPR, 2018, to third-party applications and OTT-based communication platforms as the same category of calls is treated differently depending on the platform leading to inconsistent treatment of identical communications and material consequences for consumers, including exposure to fraudulent communications, loss of trust in legitimate enterprise communications, and reduced effectiveness of regulatory safeguards.

d) That designated number series for commercial communications are also being misused for sending UCC. The regulation undermines consumer protection, reduces user choice, and creates a regulatory safe harbour for misuse of designated number series.

e) That regulation 34A is likely to defeat its own objective by weakening consumer protection, encouraging misuse of designated number series, and adversely affecting innovation and investment in consumer-protection technologies.

f) That the commercial communications should not be excluded blindly from being blocked. Request TRAI to find a way to work with applications that have provided useful services to users for many years.

g) That it is the violation of the right to privacy (right to be let alone), freedom of expression, and protection against arbitrary state action under Articles 14, 19, and 21 of the Constitution.

h) That the proposed amendment amounts to subversion of consumer choice. Section 2(9) of the Consumer Protection Act, 2019 guarantees consumers, the right to be informed and the right to choose. Consumers thus actively exercise this right by choosing to use call management applications to identify and filter unwanted communication. Therefore, the retention of Regulation 34A could have implications for consumer rights and choice.

i) One of the stakeholders has suggested to add a proviso to 34A(1) as follows: "Provided that consumers shall have the freedom to block calls Originating from any number series on their own device, at their personal discretion, and such individual action shall not affect the settings, preferences or experience of any other user's device."

j) Some of the stakeholders have commented to prohibit app-tagging for all DLT-registered CLIs, regardless of the series and all calls from registered Sender/Telemarketer numbers — not just those from designated series for commercial communications.

B. Analysis and Conclusion:

i. Regulation 3 of the Regulations mandates that any commercial communication through telecommunication network must takes place only using registered headers or the number resources allotted to the Senders from special series assigned for the purpose of commercial communication. It may be noted that the designated number series for commercial communication are allotted by the Central Government as per the National Numbering Plan, in exercise of its powers under the Telecommunications Act, 2023. Accordingly, commercial SMS can be sent only using registered headers while promotional calls can be made by Senders using number resources from 140xx series only. The Authority has also mandated use of 1600xx series numbers for service and transactional calls by entities of BFSI sector, and for government to citizen communications and 1601xx numbering series for Service and Transactional Voice Calls by entities in sectors other than BFSI and government sector.

ii. The Regulations also provide for registration of preferences by the customers on the DLT platform of the Access Providers to enable them to block or allow promotional calls from 140xx series numbers. Moreover, the Regulations also provide a comprehensive mechanism vide regulation 25 to address customer complaints

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

about unsolicited commercial communications (UCC) including any complaints related to misuse of any headers or number resources from designated series for sending UCC. There are several means such as TRAI DND app, call or SMS to 1909, mobile apps and websites of the service providers etc using which a customer can make complaint against UCC. The Regulations further provide for action against the Senders of UCC that includes suspension, barring of outgoing services, disconnection of all the telecom resources of the Sender across all the Access Providers and even blacklisting,

iii. Therefore, it is clear that the regulatory framework provides the necessary mechanism for legitimate commercial communications which are essential for the economy while at the same time, provides for measures to prevent the misuse of designated telecom resources for sending UCC. Such measures have been taken to balance the need for the protection of consumers from UCC with the need of businesses for legitimate commercial communications.

iv. Flagging of the calls from designated series numbers as spam by some call management apps or similar services appears to reflect lack of appreciation of the regulatory rationale and consumer-interest objectives underlying the Authority's framework for designated number series. For example, a customer receives calls from 140xx series only when the customer has not registered the preference to block such calls. As an opt-out mechanism is followed under the regulatory framework, such calls from 140xx series can't be termed as spam - the customer need to register the preferences to stop such calls, otherwise, consent of the customer is deemed to exists for receiving these calls. Classification of genuine business communications as spam, without adequate verification, can influence consumer perception and decision-making, potentially resulting in consumers disregarding communications that may be relevant or beneficial to them. Any tagging or filtering of calls from 140 series numbers is not allowed except for blocking on the DND registry, as any tagging of calls from 140 series numbers can mislead others customers who have otherwise allowed receipt of such calls from a sector on the DND registry. Therefore, such tagging becomes detrimental to legitimate commercial communications when a proper mechanism exists under the regulatory framework to stop these calls if so desired by the recipients.

v. Similarly, 1600xx numbering series has been mandated for government to citizen communications, and service and transactional calls by entities of BFSI sector with the key objective of making the communications from these numbers trustworthy for the customers, and also to protect the customers from financial frauds as 1600 series numbers are allotted strictly to regulated entities only. Moreover, as mentioned above, to prevent any misuse of 1600xx numbers for making promotional calls, the Regulations provide for strict action against the Senders. Flagging calls from 1600xx series numbers as spam by the CMAs and similar services would erode the trust of the customers in legitimate financial communications, thereby, leaving them vulnerable to financial frauds. Further, the Authority has observed instances where names of trusted public institutions and authorities, including TRAI, were falsely associated with certain calling numbers through crowd-sourced tagging mechanisms deployed by certain call management applications (CMAs), which may lead to frauds. Such instances not only cause serious reputational harm and erosion of public confidence in public institutions but also demonstrate that the identification systems deployed by these CMAs operate without adequate verification and accountability standards, which are susceptible to manipulation, impersonation and misuse by malicious actors.

vi. As already discussed in the EM, the Authority has also issued a Direction on 10th August, 2026 for the operationalisation of 1601xx in a phased manner, covering Utilities, Logistics and Courier services in first phase. Again, service and transaction calls from such entities are important for the customer, and any tagging or filtering of such calls may create inconvenience for the customers by conveying misleading information about the nature of these calls.

vii. The comment of some of the stakeholders that the Authority is extending its jurisdiction beyond its domain is ill founded. The number resources have been defined under the Telecommunication Act, 2023, vide sub-section 2(r) as follows:

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

"2 (r) "telecommunication identifier" means a series of digits, characters and symbols, or a combination thereof, used to identify uniquely a user, a telecommunication service, a telecommunication network, elements of a telecommunication network, telecommunication equipment, or an authorised entity;"

viii. Moreover, sub-section 3(8) of the Telecommunication Act, 2023 provides for the allotment of telecommunication identifiers to the authorised entities by the Central Government:

3 (8) The Central Government may, subject to such terms and conditions, including fees or charges as may be prescribed, allot telecommunication identifiers for use by authorised entities.

ix. Under Section 11(1)(b)(v) of the TRAI Act, 1997, the Authority is mandated to lay down standards of quality of service to protect the interests of consumers of telecommunication services. A combined reading of the relevant provisions of the Telecommunication Act, 2023 and the TRAI Act, 1997 indicates that the assignment and use of telecommunication identifiers, including number resources, constitute licensed activities under the Telecommunication Act, 2023. Since the integrity, authenticity and proper usage of such identifiers directly impact the quality, reliability and trustworthiness of telecommunications services received by consumers, their management forms an integral part of the Quality of Service framework, and, therefore, falls within the regulatory domain of the Authority. Therefore, the argument that TRAI does not have the jurisdiction, does not stand.

x. Accordingly, since the TCCCPR, 2018 regulates commercial communications as an integral component of the overall quality of service framework, call management applications (CMAs) or similar services must not provide functionalities that operate in a manner inconsistent with the provisions of the Regulation. It is established law that any contractual provision in contravention of any existing law, rule or regulation is void to the extent of such contravention. Hence, the CMAs or similar services cannot provide any feature which is in contravention of any existing law, rule or regulation. The regulatory framework seeks to ensure that the treatment and classification of commercial communications carried over telecom networks at app-layer do not undermine the intended purpose of designated telecom numbering series prescribed for commercial communications. Such safeguards are essential for maintaining consumer trust, ensuring effective delivery of legitimate communications, and preserving the quality of telecommunication services while advancing consumer protection objectives.

xi. One of the stakeholders has commented that the amendment amounts to subversion of consumer's choice to identify and filter unwanted communication. However, the fact is that regulation 34A does not prohibit a consumer to identify or filter unwanted communication for his/her own purpose, and the customer is free to do so at his/her device level for the incoming calls. What 34A prohibits is that based on crowd sourcing i.e. flagging or reporting of calling numbers as spam by certain recipients, the app or similar service itself will not flag the incoming calls Originating from any number series designated for commercial communications by the Authority, displaying as spam or such other tag to all the recipients. Further, to bring more clarity, a proviso has been added to the sub-regulation (1) of 34A to this effect.

xii. With regards to the comment of some stakeholders to prohibit app-tagging for all DLT-registered CLIs, regardless of the series and all calls from registered Sender/Telemarketer numbers, it is pertinent to mention that Regulation 3 of the Regulations mandates commercial communication only using registered headers or the number resources allotted to the Senders from special series assigned for the purpose of commercial communication. Accordingly, as far as promotional calls are concerned, 140xx series has already been mandated for use by all the registered Senders and Telemarketers. Besides, 1600xx series has been mandated for service and transactional calls by the entities in the BFSI sectors and 1601xx numbering series for Service and Transactional Voice Calls by entities in sectors other than BFSI and government sector. Considering the key advantages of using special series, which include ease of technical implementation as well as easier identification of the commercial communications by the recipients, the Authority is of the opinion that

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

designating special series for commercial communications is the right approach, and as and when any series is designated for service and transactional communications of the other sectors, regulation 34A would be applicable to it.

xiii. However, the Authority is also of the view that service and transactional calls from different sectors may require different regulatory treatments for example, based on the criticality of the communication, nature of the sector, its importance to economy etc. Accordingly, a proviso has been introduced that the Authority may specify different treatment by call management applications or similar services for different designated series for commercial communications from time to time.

C. Stakeholders' Comments on sub-regulation 34A (2)

The stakeholders commented as below:

a) That the regulation compels disclosure of proprietary data, including user-generated intelligence and behavioural analytics developed through significant investment, amounting to an unconstitutional deprivation of property under Article 300A

b) That the mandatory requirement to transmit user-generated reports to the DND registry wrongly equates user-generated tags with formal complaints, even though such tags are merely indicative signals and do not meet the regulatory requirements of valid complaints.

c) That the mandate is contrary to Article 300A of Constitution and also imposes unreasonable restriction on their fundamental right to carry on a trade or business. Creates an onerous need to build new infrastructure and undertake costly product integrations.

d) That privacy and audit requirements may be added such as data minimization for reports, user notice/consent for forwarding reports, an API standard for forwarding to DND registry, and requirement of periodic compliance audits.

e) That the Words "to the DND registry maintained by the Access Providers" be replaced with "to the DLT platform maintained by the Access Providers, in such structured format as the Authority may specify, so as to enable corroboration with the data generated under Regulation 21A and the complaints recorded under Regulation 25."

f) That 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.

g) That following proviso may be added: 'The Call Management Applications should ensure spam tagging by consumers and its data retention, through non-repudiable systems and processes. The Authority can conduct audit of said systems/processes either directly or through 3rd parties appointed by it'.

h) That with respect to Clause 34A(2), it is submitted that the DND registry maintained by Access Providers is structured and operates within a defined framework. The existing system architecture is not designed to receive or process inputs from phone diallers or third-party applications.

i) That the user-generated reports or tags from such platforms do not constitute verified complaints; they are merely crowdsourced signals. Routing such unverified inputs at scale would dilute the effectiveness of the current DND and complaint redressal mechanism.

j) That it also introduces a significant risk of false positives, with no established mechanism for verification or withdrawal (de-registration) of such reports. Therefore, the inclusion of unverified complaints and reports, without prior pilot testing or impact assessment, is not justified.

k) That without prejudice to the above, TSPs should not be penalised for any complaints received through such unverified channels.

l) That the application providers fall outside the telecom regulatory scope of Access Providers, compliance requirements such as reporting formats, data transmission, and accuracy should be directly assigned to the respective application providers.

m) That prolonged inaction has enabled them to continue operations that adversely impact the reputation and trust of legitimate enterprises. At present, no defined mechanism exists for coordination with or reporting to the concerned Ministry. It is requested that the Authority establish a formal process for reporting, inter-agency coordination, and time-bound enforcement action.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

D. Analysis and Conclusion

i. The regulation requires that the spam reported through the call management apps by the customers should get reported on the DLT platform maintained by the Access Providers. This is required because action can be taken by the Access Providers against the telecom resources of the spammers only if the spam complaints/reports are registered on DLT platform. Considering that recipients of the commercial communication many times may have a tendency to report spam/UCC on the phone dialler app itself or any call management app they are using as per their choice, this measure is necessary as increased reporting on the DLT platform of Access Providers leads to faster identification of the spammers and quicker action against them as per the regulations.

ii. However, it is observed that the complaint reporting on the DLT platform of the Access Providers is low compared to number of communications flagged as 'spam' by AI/ML based UCC detect system. Another issue inferred during interactions with the consumers in consumer awareness programs, etc., is that many consumers are reporting spam on call management apps including phone diallers and third party apps, which provide functionalities to enable the users not only to tag and block communications as spam or fraudulent, but also to "report" such communications in a manner that creates an impression that such reporting would result in enforcement action against the spammer. However, such applications neither possess statutory Authority nor institutional capability to undertake regulatory enforcement action against misuse of telecom resources. Due to non-action against reported spam, it not only creates confusion among customers about proper reporting of the spam but also lowers public trust in established institutional mechanisms.

The concern is evident from the following facts:

(a) As per the information provided by the Access Providers, in the month of April-2026, about 771 crore calls and 48 crore SMS were flagged as suspected spam by the AI systems of the TSPs for alerting customers. Also as per a report, Truecaller has claimed that 4,168 Crore spam calls and 12,903 Crore spam messages were identified in the year 2025 which comes to about 347 Crore spam calls per month and 1,075 crore spam messages per month. However, the number of complaints made by the customers on the DLT platform of the Access Providers in the month of April 2026 is only 3.65 lakh (approx.). This highlights a significant gap in the reporting of UCC complaints on the appropriate platform, where effective enforcement action can be taken against the Sender.

(b) It is also pertinent to mention while the Truecaller report mentions that 1189 crore unwanted calls were blocked in 2025, which is about 99 Crore calls per month, such blocking is user specific and that too against individual numbers only, not against the Sender as a whole who may possess many calling numbers. Simply blocking a number at the call management level on a device does not help in controlling UCC as UCC Senders keep on changing the numbers frequently. Consequently, the absence of systematic reporting of spam by call management applications and similar platforms is resulting into a considerable gap between reports-available for regulatory analysis and actual reports/complaints being reported on DLT platform. This point is evident from the data provided by the Truecaller report which mentions that number of most calls by one spammer in the year 2025 is more than 1.25 crore and that that the spammer was reported more than 3.25 lakh times during the same period. It shows that despite reporting of the spammer by the recipients for more than 3.25 lakh times on a call management app in one year, the spammer could not be prevented from sending UCC, who made about 1.25 crore calls during 2025 i.e. more than 34 thousand calls per day.

(c) The Authority, under the TRAI Act, 1997, regulates the commercial communications through TCCCPR 2018. CMA apparently establish a parallel regime which creates an impression among the customers that reporting of UCC through the CMA would result in enforcement action, whereas, in reality, such reports cannot trigger the statutory processes and enforcement measures envisaged under the TCCCPR-2018.

(d) Therefore, the above facts establish that reporting of UCC only at the regulated DLT platform of the Access Provider is necessary to tackle the menace of UCC effectively.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

iii. The concern raised by one of the stakeholders that the regulation compels disclosure of proprietary data, including user-generated intelligence and behavioural analytics, amounting to an unconstitutional deprivation of property under Article 300A, is unfounded as the regulation does not mandate sending any proprietary data prepared after carrying out behavioural analytics by the CMAs. The regulation only mandates that reporting of any call or SMS as spam by the consumers, without applying any algorithm etc for behavioural analytics, and which, therefore, does not constitute any proprietary data, shall be transferred to the DLT Platform. Accordingly, the sub-regulation 34A (2) merely requires the CMAs to send, in a standardized format, only such details to the DLT platform of the Access Providers, which are contained in the customer's report about the reported communication, without the need of any further analytical processing by CMAs, so as to enable regulatory action against UCC. Further, it also addresses the issue raised by one of the Access Providers that the existing system architecture is not designed to receive or process inputs from phone diallers or third-party applications. The data will be sent by CMAs to the Access Providers as required under first proviso to sub-regulation 23 (5) only. Although, initially, under the draft regulations, it was envisaged to treat such data as complaints yet considering the complexity involved, it is decided that the Access Providers shall treat such data as reports and use it as an input for identifying suspected spammers based on behavioural analysis.

iv. Regarding the comment of a stakeholder that the regulation imposes unreasonable restriction on their fundamental right to carry on a trade or business, it is to be noted that regulation does not seek to regulate Internet-based applications generally - it merely mandates safeguards necessary to preserve the identity of designated commercial communication series, and ensure proper handling of UCC-related reports within the regulated telecom ecosystem. The regulations aim to ensure that large-scale identification and tagging of UCC, operate within appropriate regulatory guardrails, and, therefore, cannot be construed as imposing unreasonable restrictions.

v. It is obvious that the business of any CMA that offers reporting and tagging of spam/ UCC and also whitelisting certain flagged Senders, runs around the existence of UCC. As the spam reported to various CMAs is presently not being reported at the DLT platform where regulatory action can actually be enforced, such UCC Senders continue to send UCC unhindered. Therefore, it becomes necessary that any CMA that is interested in protecting consumers from spam, should forward the reported spam communications to the DLT platform to enable enforcement against the UCC Senders.

vi. On the comments by stakeholders that the process implemented by these entities (CMAs) should be non-repudiable and that check on the veracity of the information basis which action is expected from TSPs, should also be ensured, the Authority notes that no direct action by the TSPs against the Senders, solely on the basis of the information reported by the CMAs, is being envisaged as of now, and the Access Providers shall use the reported data as an input for identifying suspected spammers based on behavioural analysis.

E. Stakeholders' Comments on sub-regulations 34A (3):

The stakeholders commented as below:

a) The automatic deeming of non-compliance and lack of adequate procedural safeguards adversely impact the operational freedom of private enterprises and impose disproportionate regulatory burdens on entities outside TRAI's regulatory framework.

b) Require clear user notice that "report spam" will be transmitted to operators/DLT and specify minimum data fields and opt-out of sharing contact list.

F. Analysis and Conclusion

i. In view of the detailed analysis above, to effectively control UCC, it is essential that the call management apps including phone diallers and third party apps, or similar services comply to the regulatory provisions. On the comment of a stakeholder regarding "deeming of non-compliance" under sub-regulation (3), it may be seen that the proviso to the regulation provides adequate procedural safeguards that any order for initiating action under sub-regulation (3) shall be made by the Authority, only after the concerned entity has been given a reasonable opportunity to represent.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

ii. As far as action for non-compliance under applicable laws is concerned, the Authority notes that under Section 79 of the IT Act, 2000, an intermediary has exemption from liability of intermediary if the intermediary observes due diligence while discharging his duties under this Act, and Rule 3(1) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, specify the due diligence to be observed by the intermediary, which includes 3(1)(d) as reproduced below:

"(d) an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force."

iii. Sub-section 79(3)(b) of the IT Act, read with Rule 3(1)(d) of the IT Rules, 2021 enable an authorised agency of the appropriate Government to issue notices to IT intermediaries for violation of any law. As regulations issued by TRAI are subordinate legislation, any violation of the regulations of TRAI by the call management apps is covered under the Rule 3(1)(d), and attracts Rule 7 of the aforesaid IT Rules, 2021, which provides for the action against the intermediary for non-observance of the rules, and is reproduced below:

"7. Non-observance of Rules.—Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code."

19. Amendments to Regulation 35

i. The extant proviso to regulation 35 provides exemption to the Central Government, the State Government and the bodies established under the Constitution from Service SMS charge for their own purpose. To reflect this, the words "by or on the directions of" in items (i) and (ii) of the proviso have been substituted with the words "by or on behalf of".

ii. The rationale behind new proviso, inserted before the existing proviso, has already been discussed under the section on A2P calls.

20. Registration of Senders/ Telemarketers: Amendment to Schedule-I

A. Stakeholders' Comments:

a) One stakeholder suggested alternative methods of verification and authentication should maintain assurance standards equivalent to physical or biometric verification. It was suggested to incorporate digital identity assurance levels, fraud prevention mechanisms such as SIM change/port checks, and privacy-by-design safeguards. This is to future-proof the regulatory framework in view of evolving e-KYC and remote onboarding practices, while ensuring adequate safeguards against fraud, misuse, and UCC, without creating barriers for legitimate MSMEs and rural entities.

b) A few stakeholders proposed GST-verified digital KYC for cloud-based and remote entities as an alternative verification mechanism, since physical verification is difficult for digitally operated and work-from-home enterprise models. It is aligned with the Government's digital KYC initiatives such as Aadhaar e-KYC, DigiLocker, and CKYC which is equivalent to physical KYC.

c) Two stakeholders suggested that the manner of verification and authentication should be formulated after consultation with TSPs and other stakeholders to ensure feasibility of implementation and alignment with the existing norms.

B. Analysis and Conclusion

i. Item 1(4) of the Schedule-I provides for physical verification and biometric authentication of the Senders before registration by the Access Providers. The provision limits the method of verification to physical

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

verification only and that of authentication to biometric authentication only. However, there may be a need to modify these methods based on the latest technological developments, the scale of operation of Sender/ Telemarketers etc. Accordingly, a proviso has been introduced for specifying different/ additional methods of the verification and authentication of the entities.

21. Messages to be sent in relation to 'consent': Amendment to Schedule-I

A. Stakeholder's Comments

a) Ensure that short code 127xxx, or any other code/header as prescribed by the Authority, shall be used by all Access Providers for sending consent related messages and that the words 'or any other code' should be modified as 'or any other code/SMS headers'

B. Analysis and Conclusion

i. In view of the modified definition of 'Explicit Consent' which permits onboarding of legacy consent, the scope of messages to be sent to the customers using short code has been widened from only 'consent seeking messages' to all the 'consent related messages'.

ii. The Authority agrees to the suggestion of the stakeholder for substituting the words 'or any other code' with the words 'or any other code/SMS headers' as based on the requirements, sending messages by the Access Providers under Consent Registration Function may need to be allowed through other SMS headers also.

22. Amendments to Schedule II in relation to Preference category etc.

A. Stakeholder's Comments

a) In relation to migration of all preferences registered under FULLY BLOCK category to BLOCK PROMO category, it was suggested to provide that during this period, the Access Provider shall notify all affected subscribers that their 'Fully Block' preference will be converted to 'Block Promotional' and that transactional and service-type commercial communications will no longer be blocked under this preference setting.

B. Analysis and Conclusion

i. Item 1(1) of Schedule II provides for blocking various categories of promotional commercial communications (CC) as well as blocking all the promotional communications as per the preferences of the customer. However, as per Note 3 to the item, transaction type CC are not blocked. Considering the fact that service type CC are either linked to the transactions done by the customers e.g. balance alerts, flight delay info, product updates etc., or sent to the customer based on the existing Relationship between the Sender and the customer, such communications require same treatment as given to transactional type of commercial communications. Similarly, government communications, being in the interest of the citizens and sometimes critical e.g. disaster warning, also require treatment similar to that for transactional type CC. This amendment, accordingly, provides for not blocking service type CC as well as government communication, as is done for transactional type CC. Moreover, as service type of commercial communication based on explicit consent are essentially promotional commercial communications, this differentiation is being removed, and such communications will be treated as promotional commercial communications based on explicit consent of the customers.

ii. In line with the Item 1(1) of Schedule II, same treatment for transactional type CC, service type CC, and government communication is stated in respect of 'time allowed for delivering commercial communication'. No time restrictions have been included for delivery of these types of communications as they are crucial for the customers. For example, an alert about a flight delay information needs to be conveyed to the passenger as soon as the same is announced by the airline.

23. LRN update in case of number porting: Amendment to Schedule II

A. Stakeholder's Comments: No comments were received.

B. Analysis

iii. Sub-item (2) (b) of item 6 of Schedule II of the regulations mandates the Access Providers to record the Location Routing Number (LRN) of the current serving network of the customer and also changes in LRN of the new serving network, in case customer is being ported-in during Mobile Number Portability. The update in LRN is necessary in case of MNP as this enables the transfer of existing preferences and consents of the customer over the DLT, and

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

makes it possible for the customer to register for DND services and change their preferences and consents seamlessly. TRAI direction dated 9th June, 2025, mandated that the Location Routing number (LRN) of the Recipient Network for the ported-out customers has to be updated in the DLT system by Donor Access Provider within 24 hours of successful porting transaction. However, feedback has been received from the industry that even after customer is ported out, LRN is not being updated timely by Donor Access Provider, and this creates problem for the customer to record and change his/her preferences and consents. To remove this operational problem and considering the fact that under the MNP regulations, recipient operator becomes the authoritative source for the number's current routing and service profile after successful porting, an amendment to sub-item 2 (b) of the item 6 of Schedule II has been introduced that the LRN has to be updated by the recipient Access Provider within 24 hours after successful porting transaction.

24. Intimation to the suspected Senders of UCC: Amendment to Schedule IV

A. Stakeholders' Comments:

a) Some of the stakeholders commented to delete the proposed amendment as it may require suitable refinements to ensure alignment with the industry's operational realities and the intended regulatory objectives.

B. Analysis and Conclusion

i. The Authority observes while Access Providers have started alerting the recipients about the suspected UCC, the Senders suspected of sending UCC do not get any alert that the communication being sent by them is being flagged as suspected spam/UCC. The Authority is of the view that there is a need to alert such Senders also so that they can take corrective action and refrain from sending UCC. Accordingly, an amendment to this effect has been done in item 1, sub-item (4) of Schedule-IV.

25. Issues raised in relation to commercial communications sent by the Senders through VNOs: Amendment to Regulation 13

A. Stakeholders' Comments:

a) VNOs (Virtual Network Operators) should be recognized as distinct entities for which separate criteria may be prescribed, considering their specific role in the ecosystem.

b) It was commented that VNOs should be explicitly authorized to register legacy consents on behalf of their Sender clients through the NSO-operated Consent Register Framework portal, using the VNO's unique Licensee ID and NSO provided access to DLT platform.

c) One stakeholder cited technical and operational challenges in declaration of A2P calls where a VNO acts as an intermediary.

d) Requested clarification that the five-business-day reply window should commence from the time of intimation to the Sender and proposed mandatory simultaneous notification to the concerned VNO through the NSO so that the VNO can investigate records and submit evidence. It was further suggested that, for VNO customers, blocking or suspension actions should be undertaken by the VNO rather than the NSO, since NSO don't have the visibility of the client.

e) It was also commented to exempt A2P Charges for VNOs as VNOs have bilateral one-to-one commercial agreements with TSPs, and cost recovery is already governed by the commercial contracts. A regulatory charge creates a "double-tax" on AGR-paying entities.

B. Analysis and Conclusion:

i. The Authority observes that the definition of "Access Providers" as per sub-regulation 2(b) specifically includes a Virtual Network Operator (VNO). Accordingly, VNOs are subject to the regulatory obligations prescribed under the Regulations, and there is no need to categorise them as entities distinct from Access Providers. However, to meet the regulatory obligation, access to the Distributed Ledger Technology (DLT) platform is required, which is presently maintained by TSP/NSO.

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

ii. As far as comments related to registering legacy consents and declaration of A2P calls on DLT platform, and various flows under complaint mechanism are concerned, the Authority notes that these issues are coming up primarily due to non-availability of a proper interface to VNOs with DLT platform using which they can smoothly perform various obligations as Access Providers under the regulations. They presently rely on alternative means such as exchange of mail with the NSOs to get the necessary action done at DLT level. Since, as per the terms and conditions of the VNO license, they are not permitted to have direct interconnection with any Access Provider other than their parent NSO, while becoming part of DLT platform necessarily involves direct interconnection with all the participating Access Provider, the Authority is of the view that there is a need for the parent NSO to offer the VNO a digital interface which must have real time functionality with DLT platform and any other systems so as to enable the VNO to perform its obligations under these regulations. If deemed appropriate, the Authority may also specify such mechanism from time to time. Accordingly, provisions to this effect have been introduced in the regulation 13.

iii. Regarding exempting A2P Charges for VNOs, the Authority observes that A2P charges have been provisioned to act as a deterrent against UCC, and not as a cost recovery mechanism. Accordingly, there should not be any exemption for VNOs on the grounds of cost recovery.

26. Issues raised in relation to commercial communications sent by the Senders through Cloud Communication Platforms (CPaaS):

A. Stakeholders' Comments:

a) It was commented that Registered Cloud Communication Platforms (RCCPs) should be recognized as distinct entities for which separate criteria may be prescribed, considering their specific role in the ecosystem.

b) A stakeholder submitted that suitable provisions should be incorporated within the DLT ecosystem enabling CPaaS operators to furnish KYC details, with the consent of the Sender, where their resources have been flagged.

c) It was suggested where a Sender is served through a Registered Cloud Communications Platform (RCCP) or other registered intermediary, the OAP should simultaneously notify such platform/intermediary of the complaint details, excluding complainant identity, to enable faster investigation and action against violating Principal Entities. Also, that RCCPs are operationally best placed to identify the responsible PE, examine consent/CDR records, disable access of violators, and support coordinated enforcement with appropriate privacy safeguards.

d) One of the stakeholders proposed to introduce a three-business-day pre-suspension representation window for Senders and CPaaS providers.

e) It was also suggested to normalise the complaint threshold based on the total number of channels/resources, stating that high-volume CPaaS trunks hit low thresholds through statistical false positives.

B. Analysis and Conclusion:

i. The Authority notes that under the regulatory framework, the Registered Cloud Communication Platforms (RCCPs) act as Senders/ aggregators. Moreover, it has also been learnt that for the purpose of making commercial calls, it is the RCCP who make outgoing calls to the recipient as well as to the Sender using it's own telecom resources, and then bridges them to make the communication through between the Sender and the recipient. Under these circumstances, the RCCP cannot be treated at par with an Access Provider, and accordingly must meet the obligations as a Sender/ aggregator.

ii. As far as introducing a different threshold for high-volume CPaaS traffic is concerned, in case a justified need arises for such differentiation, the provisions for classifying Senders and differential regulatory treatment for such classes have already been discussed elsewhere in the explanatory memorandum.

27. The Authority received an additional comment suggesting amendment to sub-item 2, item 2 of Schedule-I that the Access Provider shall ensure that the name of the Principal Entity (PE) is displayed to the recipient for all calls

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi

Originating from the 140/1600 numbering series. The aforesaid item *inter alia* provides that the headers assigned to the Senders for the purpose of making commercial voice calls shall include Calling Line Identity for Senders making commercial voice calls from any numbering series directed by the Authority/DoT. In this regard, the Authority notes as per Telecommunications (Authorisation for Provision of Principal Telecommunication Services) Rules, 2026, effective since 23rd June, 2026, the definition of CLI as per Rule 2(1) (j) states that "calling line identification" means— (i) the telecommunication identifier assigned to a calling user by the new authorised entity or licensee providing telecommunication service to such user; (ii) the name of the user as recorded in the subscriber data record; or(iii) such other identification as may be specified on the portal;". Therefore, the Authority is of the view that this definition already takes care of the comment regarding display of the name of the entity as per subscriber data record.

18/09/2026

हरिन्द्र कुमार/Harinder Kumar, ITS
सचिव/Secretary
भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India
नई दिल्ली/New Delhi