

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

S. No	Regulation No. /Provision	Sub Regulation/ Item No,	Modification proposed to the draft amendment	Reasons/full justification for the proposed modifications	Remarks/ Observation BSNL
(1)	<b>1. Short title, extent and commencement</b> These regulations may be called the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 (... of 2026).	(3) These shall come into force after <b>thirty days</b> from the date of their publication in the Official Gazette.			
(2)	<b>2. Definitions - In these regulations, unless the context otherwise requires</b>	after clause (e) <sup>1</sup> the following clause shall be inserted, namely; <i>“(ea) An A2P (Application-to-Person) call refers to a voice call that is initiated by an application, software system, or automated platform without direct human dialling and delivered to an individual telecom subscriber, including using autodialling, robo-calls and/ or prerecorded/ artificial voice technologies.”</i>	The definition of A2P calls seems to be OK.		However, BSNL does not have the information as of now whether the customer is going to use the service for manual dialling or auto dialling, be it LL, SIP/PRI, FTTH, Mobile, VoIP etc.
(3)		for clause (y), the following clause shall be substituted, namely: - <i>“Explicit Consent” means such consent which has been either verified directly from the Recipient</i>	No change		

		<i>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.”</i>			
(4)		in clause (ai), for the words “clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885)”, <del>the clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885);</del> words “clause (g) of section 2 of The Telecommunications Act, 2023 (44 of 2023)”, shall be substituted;	<b>No change</b>		
(5)		for clause (ba), the following clause shall be substituted, namely:- <del>means specifically constructed experimental space, with a safe environment, within which various stakeholders can use Regulatory Technology solutions to develop and refine Code(s) of Practice to comply with new regulatory requirements;</del> “(ba) “Regulatory Sandbox” means a live testing environment where new products, services, processes, regulatory technology solutions and business	<b>No change</b>		

		<p>models may be deployed for a limited set of eligible customers, for a specified period of time, with certain relaxations in the extant regulatory provisions in order to encourage and facilitate innovation and technological development in telecommunication; development and refinement of Code(s) of Practice; and provide inputs for regulatory interventions and modifications.”</p>			
(6)		<p>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, <del>ii. on the basis of the purchase or transaction made by or done by the recipient with the sender within the twelve months immediately preceding the date of the communication; or</del> (ii) on the basis of <del>inquiry or</del> application regarding products or services made by or submitted by recipient to</p>	<p><b>The mentioned clause may be simplified as:</b></p> <p>“<b>Relationship</b>” means there is already some business connection between a person or entity and a subscriber</p> <p>This can happen in 2 ways:</p> <ol style="list-style-type: none"> <li>1. Business connection If they are connected for business reasons, with or without payment.</li> </ol>	<p><b>The suggested clause is providing the information clearly.</b></p>	<p>- The Authority is requested to provide more clarification on the proposed deletion of ‘inquiry’.</p>

		<p>sender within the three months immediately preceding the date of the receiving of communication, which relationship has not been previously terminated by either party;"</p> <p><del>(iv) for social reasons, between a person or entity and a subscriber with or without an exchange of consideration, by voluntary two-way communication, initiated from both sides at different points in time;</del></p>	<p>2. If the person asked about or enquired or applied for a product/service in the last 3 months, and neither side has ended the connection.</p>		
(7)		<p>in clause (bh), (i) its Customer or Subscriber to provide information pertaining to any product or service, its warranty, product recall, software upgrade alerts, safety or security of the product used or purchased by the Customer, periodic balance alerts, information regarding delivery of goods or services, and such messages or voice calls are not promotional in nature and do not require Explicit Consent; or (ii)a Recipient to facilitate or complete a commercial transaction involving the ongoing purchase or the use by the Recipient of the product or services offered by the Sender after obtaining Explicit Consent from the</p>	<p><b>No change</b></p>		

		Recipient and such messages or voice calls are not promotional in nature:			
(8)		clause (bn), “Subscriber” means a person or legal entity who subscribes any service for telecommunication <del>to a telecom service provided by an Access Provider;</del>	No change		
(9)		clause (bo), “Telecom resources” means any <del>telegraph</del> telecommunication equipment and/or telecommunication identifier, as defined under The Telecommunications Act, 2023 (44 of 2023) used to send voice call or messages;	No change		
(10)		clause (bw), “Unsolicited commercial communication or UCC” means any commercial communication that is neither as per the consent nor the registered preferences of the Recipient and does not include: - <del>Any transactional message or transactional voice call;</del>	No change		
(11)	3.: Commercial communications through network of Access Providers. —	(1) Every Access Provider shall ensure that any commercial communication using its network takes place only using registered	No change		

		<p>headers or the number resources allotted to the Senders from special series assigned for the purpose of commercial communication. “Provided that Authority may classify the senders for this purpose and may specify different criteria for different classes of senders.”</p>			
(12)	<p>4, Intimation regarding use of A2P calls <del>Auto-Dialer or Robo-Calls.</del> — Every Sender shall declare to notify the Originating Access Provider, in advance, about the use of Application-to-Person (A2P) calls. <del>Auto-Dialer or Robo-Calls as well as the intended objective of such calls in writing.</del> . Provided that any such call made by a sender without prior declaration to the OAP, shall be treated as unsolicited commercial communication (UCC), and the OAP shall take action against such sender as per the provisions of these regulations.”</p>		<p>Intimation regarding use of A2P calls <del>Auto-Dialer or Robo-Calls.</del> — Every Sender shall declare to notify the Originating Access Provider <b>on DLT</b>, in advance, about the use of Application-to-Person (A2P) calls. <del>Auto-Dialer or Robo-Calls as well as the intended objective of such calls in writing.</del> . Provided that any such call made by a sender without prior declaration to the OAP, shall be treated as unsolicited commercial communication (UCC), and the OAP shall take</p>	<p><b>Declaration is to be given in DLT, since TRAI has already suggested to register all the SIP/PRI on DLT, during the registration process PE can declare the A2P use of the resources, if declared on DLT the same will be helpful while attending the UCC complaints,</b></p>	

			action against such sender as per the provisions of these regulations.”		
(13)	11. Every Access Provider shall give due publicity through appropriate means to make the customers aware regarding:	4. Every Access provider shall inform its Subscribers while giving telecom resources that he shall not get involved in the activity of sending Commercial Communication or cause sending Commercial communication, or authorize the sending of the Commercial Communication using the telecom resources failing which the telecom resources used or assigned to him may be <del>put under Usage Cap or his telecom resources may be</del> disconnected;	<b>No change</b>		
(14)	21A. For taking action against the senders suspected of sending unsolicited commercial communication, as detected by the AI/ML-based UCC_Detect system established by the access providers in accordance with Schedule IV, every access provider shall implement the following :-	(a) Every Terminating Access Provider (TAP), shall, through its AI/ML-based UCC_Detect system, identify and flag the Calling Line Identification (CLI) of the sender as “Suspected UCC CLI” based upon the behavioural parameters as specified in the AI/ML-based UCC_Detect system, and immediately upon such flagging and in any case within two hours of such flagging, share, through the	<b>The clause to be appended with “If the OAP is not identified by the system for the suspected SPAM number or the identified OAP says the mentioned number does not belong to the OAP, TAP may report the such numbers to TRAI</b>	<b>There are many cases where the OAP is not identified for the number detected as suspected SPAM, clear guidelines are not included in the amendment for such cases.</b>	

		Distributed Ledger Technology (DLT) platform, the flagged CLI with the concerned Originating Access Providers (OAPs);	<b><i>on monthly basis for further instructions. “</i></b>		
(15)		(b) upon receipt of the flagged CLI from the TAP, every OAP shall immediately issue a notification through SMS or mail or both, to the sender associated with such CLI, informing that based on communication behaviour, the CLI has been flagged as suspected of sending UCC (spam)”; Provided that the authority may prescribe the format and manner of sending such notification from time to time.			
(16)		(c) OAP shall, within one business day of the receipt of the flagged CLI from TAP, identify unique KYC identifiers of the sender associated with such CLI, using its subscriber records, and share the same through DLT platform with all other Access Providers, who, within one business day of the receipt of such unique KYC identifiers from OAP, shall identify all the telecom resources allotted by them to such Sender;			

(17)		<p>(d) upon identification of all the telecom resources allotted to such Sender, as referred in the preceding para, all the Access Providers including OAP, shall examine, within next one business day, whether any other CLI allotted to the same Sender has been flagged as “Suspected UCC CLI” by their respective AI/ML-based spam alert systems during the preceding ten days, and all such flagged CLIs mapped to the same sender shall be recorded and shared on DLT platform by all the Access Providers on the same day;</p>			
(18)		<p>(e) upon receipt of the data of all CLIs associated with such sender across the network, which have been flagged as “Suspected UCC CLI”, all the concerned OAPs shall check, within one business day of the receipt of such data, whether five or more CLIs of the sender have been flagged as “Suspected UCC CLI” within a period of last ten days, and if it is found that five or more CLIs of the sender have been flagged as “Suspected UCC CLI”</p>	<p>Clause e.(ii) and e.(iii) may be modified as</p> <p>(ii) for the second such instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources</p>	<p><b>The action on KYC mismatch should not be same as that of misuse of telecom resources.</b></p>	<p>The Authority is requested to elaborate the definition of misuse of telecom resource.</p>

		<p>within the last ten days, all the concerned OAPs shall take action against the sender as follows:</p> <p>(i) for the first such instance, OAP shall, within the next three business days, carry out the re-verification of KYC of the sender as per the licence conditions and take necessary action in accordance with the extant KYC guidelines;</p> <p>(ii) for the second such instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the provisions of the regulations, outgoing services of all telecom resources including PRI/SIP trunks, SIMs etc. allotted to the sender shall be barred by all the Access Providers for a period</p>	<p>allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification, <b>All the resources of the senders taken in unmatched KYC to be blacklisted immediately</b>, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the provisions of the regulations, outgoing services of all telecom resources including PRI/SIP trunks, SIMs etc. allotted to the sender shall be barred by all the Access Providers for a period of fifteen days,</p>		
--	--	--	--	--	--

		<p>of fifteen days, irrespective of whether those telecom resources were actually used or not in making such communications;</p> <p>(iii) for any such subsequent instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the provisions of the regulations, OAP shall take action against the sender as provided under clause(b) of sub-regulation (6) of regulation 25 of the regulations.</p>	<p>irrespective of whether those telecom resources were actually used or not in making such communications;</p> <p>(iii) for any such subsequent instance, OAP shall, within the next five business days, carry out the physical KYC verification of the sender to ensure that the telecom resources allotted by OAP are not being misused by the sender for sending UCC and in case KYC details of the sender, available with OAP, do not match with the details obtained on physical verification <b>All the resources of the senders taken in unmatched KYC to be blacklisted immediately</b></p>		
--	--	---	--	--	--

			<p>perpetually, or if it is found that the telecom resources are being misused by the sender for sending UCC in violation of the provisions of the regulations, OAP shall take action against the sender as provided under clause(b) of sub-regulation (6) of regulation 25 of the regulations.</p>		
(19)	22 Other obligations of Access Providers	<p><del>(i) ensure that traffic from the concerned Sender shall be suspended by all the Access Providers immediately till such time, the Sender files a complaint with the law enforcement agencies under the relevant laws, and Sender reviews all its Headers and Content Templates and takes corrective measures as per the regulations to prevent misuse of its Headers, Content Templates and other relevant credentials: Provided that no action shall be taken by Access Provider unless</del></p>			

		<del>the concerned Sender has been given a reasonable opportunity of representation; (ii) ensure that, if Delivery TM is complicit in misuse of Headers or Content Templates, the Sender shall file a complaint against Delivery TM with the law enforcement agencies under relevant laws;</del>			
(20)		(a) in case of misuse of Headers and/or Content Templates,			The Authority is requested to elaborate the definition of misuse of Headers and/or Content Templates
(21)		(i) Immediately suspend the use of such misused Header(s) and/or Content Template(s) across all Access Providers as the case may be, and the OAP shall issue a notice to the sender in whose name such Header(s) and/or Content Template(s) are registered, within 24 hours of reporting of misuse to the OAP. Such suspension shall remain in force until the conditions specified under sub-clause (ii) are fully complied with by the sender.	(i) Immediately suspend the use of such misused Header(s) and/or Content Template(s) across all Access Providers as the case may be, and OAP to inform the suspension activity to the Header/Content template registrar TSP and registrar TSP shall issue a notice to the sender in whose name such Header(s) and/or Content Template(s) are registered, within 24		

			hours of reporting of misuse/Suspension to the registrar TSP OAP. Such suspension shall remain in force until the conditions specified under sub-clause (ii) are fully complied with by the sender.		
(22)		(ii) require the sender to undertake all of the following remedial actions:			
(23)		1. Reset, within 24 hours of receipt of notice from the Originating Access Provider (OAP), all access credentials including passwords, API keys and system permissions used for submission or delivery of commercial communications, which have been allotted to the sender by the access providers and telemarketers;	1. Reset, within 24 hours of receipt of notice from the registrar TSP Originating Access Provider (OAP), all access credentials including passwords, API keys and system permissions used for submission or delivery of commercial communications, which have been allotted to the sender by the access providers and telemarketers;		Timelines is required to be maintained by the sender/customer; however, 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?

(24)		<p>2. File a formal complaint with the appropriate law enforcement agency under the applicable laws, within 2 business days of receipt of notice from the OAP, clearly identifying whether the misuse arose due to—</p> <ul style="list-style-type: none"> <li>i. compromise of login credentials,</li> <li>ii. unauthorized access to systems,</li> <li>iii. misuse by an associated Telemarketer, Aggregator, or Delivery Entity, or</li> <li>iv. any other identifiable cause, to be specified by the sender; and share with the OAP a copy of the complaint filed. Provided that, if any Telemarketer is an accomplice in the misuse of Headers or Content Templates, the Sender shall file a complaint against such Telemarketer with the law enforcement agencies under relevant laws;</li> </ul>	<p>2. File a formal complaint with the appropriate law enforcement agency under the applicable laws, within 2 business days of receipt of notice from the registrar TSP OAP, clearly identifying whether the misuse arose due to—</p> <ul style="list-style-type: none"> <li>i. compromise of login credentials,</li> <li>ii. unauthorized access to systems,</li> <li>iii. misuse by an associated Telemarketer, Aggregator, or Delivery Entity, or</li> <li>iv. any other identifiable cause, to be specified by the sender; and share with the registrar TSP OAP a copy of the complaint filed. Provided that, if any Telemarketer is an accomplice in the misuse of Headers or</li> </ul>		<p>The Authority is requested to suggest on the relevant action to be taken by the TSP, if any, upon receipt of copy of FIR from the customer.</p>
------	--	---	---	--	--

			<p>Content Templates, the Sender shall file a complaint against such Telemarketer with the law enforcement agencies under relevant laws;</p>		
		<p>3. Where the Sender claims or the OAP determines that misuse occurred due to leakage, cloning, or compromise of credentials, the Sender, within next 5 business days shall mandatorily de-register all its Headers and Content Templates including those reported as misused, and get them re-registered to obtain new header and template ids using the bulk tool provided by the concerned registrar access provider(s) to the sender for this purpose; and the sender shall ensure that previously compromised identifiers are not reused;</p>	<p>3. Where the Sender claims or the registrar TSP OAP determines that misuse occurred due to leakage, cloning, or compromise of credentials, the Sender, within next 5 business days shall mandatorily de-register all its Headers and Content Templates including those reported as misused, and get them re-registered to obtain new header and template ids using the bulk tool provided by the concerned registrar access provider(s) to the sender for this purpose; and the sender shall ensure that</p>	<p><b>If the PE has applied the headers and templates in bulk, the approval of the same cannot be done in bulk manner, the approval is to be done one by one and will create unnecessary pressure of the PE on the TSP.</b></p>	<p>(1) This says that the TSP will provide bulk tool to register the headers and templates in bulk – In this regard, the Authority is requested to clarify whether this bulk registration requires the approval process as prescribed in case of individual registration?</p> <p>(2) If the verification and approval is required then registration and approval will be a time consuming task and may hamper the traffic of the sender and its services. Moreover, re-registration all the headers and templates will get new IDs and need changes at all levels of the sender like APIs, CRM etc. - In such cases the Authority is requested to clarify whether the Deregistration include all registered headers including 1400,1600 and 10 digit SIP/PRI (if registered</p>

			previously compromised identifiers are not reused;		on DLT) ?
(25)		4. (a) Conduct within 10 business days of receipt of notice from the OAP, a comprehensive review of all its registered Headers, Content Templates, Consent Templates; and (b) Intimate to the OAP whether the misuse was due to credential leakage, compromise of IT systems or any other reason, to be specified by the sender.	4. (a) Conduct within 10 business days of receipt of notice from the registrar TSP OAP, a comprehensive review of all its registered Headers, Content Templates, <del>Consent Templates</del> ; and (b) Intimate to the registrar TSP OAP whether the misuse was due to credential leakage, compromise of IT systems or any other reason, to be specified by the sender.		
(26)		iii. Where the Sender fails to fully comply with the obligations under sub-clause (ii) within the stipulated timeframe, or provides an incomplete or false intimation, all commercial communication traffic from such Sender shall be suspended by all the Access Providers until compliance is	iii. Where the Sender fails to fully comply with the obligations under sub-clause (ii) within the stipulated timeframe, or provides an incomplete or false intimation, all commercial communication traffic		

		<p>achieved to the satisfaction of the OAP. Provided that the Authority may, from time to time, prescribe any other procedures, safeguards, timelines, and conditions to safeguard the security of the commercial communications.</p>	<p>from such Sender shall be suspended by all the Access Providers until compliance is achieved to the satisfaction of the registrar TSP OAP. Provided that the Authority may, from time to time, prescribe any other procedures, safeguards, timelines, and conditions to safeguard the security of the commercial communications.</p>		
(27)	<p><b>23) Every Access Provider shall establish Customer Complaint Registration Facility (CCRF) and shall make necessary arrangements to facilitate its customers on 24 hours X 7 days basis throughout the year: -</b></p>	<p>(1), (c) to appeal to the Appellate Authority within a period of 15 days from the date of receipt of information about the resolution of the complaint when the consumer is not satisfied with the redressal of the complaint by the Access provider, or the complaint remain unaddressed, or no intimation of redressal of the complaint is received by the complainant within a period of fifteen(15) days from the date of registering complaint, whichever is earlier. The complainant shall be able to prefer</p>			

		such appeal through any of the modes specified for lodging a complaint or report under these Regulations. The Appellate Authority shall resolve and reply to such appeal within a period of fifteen (15) days from the date of its receipt. Every Access Provider shall designate a permanent employee working at senior management level as the Appellate Authority. The name and contact details of such designated officer shall be duly published at a prominent place on the official website of the concerned Access Provider.”			
(28)	24 Distributed Ledger(s) for Complaints: Every Access Provider shall establish or cause to establish Distributed Ledger(s) for Complaints (DL-Complaints) with requisite functions, processes and interfaces:	(i) <del>to record three years history of complainant with details of all complaint(s) made by him, with date(s) and time(s), and status of resolution of complaints;</del>			
(29)		“(3) to record three years’ history, complainant-wise, with details of all complaints including appeal, if any and alleged violations reported by the complainants, with date and time, and status of resolution of complaints including the			

		supporting documents used by the access providers for resolving the complaints;”			
(30)		4) to record three years history of sender(s) against which complaint including appeal, if any is made or reported with details of all complaint(s) including appeal, if any, with date(s) and time(s), and status of resolution of complaints;			
(31)	25. Complaint Mechanism: Every Access Provider shall establish systems, functions and processes to resolve complaints made by the Customers; corroborate the complaint data with the data of senders suspected of sending UCC by the AI/ML based UCC detect systems across all the access providers,; and <del>to</del> take remedial action against Senders as provided hereunder (Sender herein shall mean a sender or telemarketer, who has been allotted the telecom resource by the access provider, that has been used for making such communication, and against which the UCC complaint has been made.);-				
(32)		the Terminating Access Provider shall also verify if the date of receipt of complaint is within seven days of receiving Commercial Communication and in case the complaint is reported by the Customer after seven days, it shall communicate to the Customer about the closure of his complaint along with reasons in accordance with the Codes of Practice for Complaint Handling and change status of the complaint on DL-Complaint as a report instead of a complaint: Provided that the Authority may, if it so desires, by direction, specify the content and method of making such			

		<p>communication to the complainant;</p> <p>Provided further that every complaint reported by the customers after seven days but before the lapse of fifteen days of the receipt of the unsolicited commercial communication by the customers, shall be recorded by the terminating access provider as well as the originating access providers;</p>			
(33)		<p>4 b) examine communication detail records, within <del>one</del> 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;</p>			
(34)		<p>4 d) in case of occurrence of SMS-related complained communications under sub-regulation (4)(b), OAP shall further examine, within <del>one</del> three business days from the date of receipt of complaint by the OAP, whether all regulatory pre-checks were carried</p>			

		<p>out in the reported case before delivering Unsolicited Commercial Communications; and</p>			
(35)		<p>4 d (ii) in case of non-compliance with the regulations, within <del>two</del> <b>three</b> business days from the date of receipt of complaint by the OAP, take action against the defaulting entity and communicate to TAP to inform the complainant about the action taken against <del>his</del> <b>the</b> complaint as provided for in these regulations and Codes of Practice: Provided that the Authority may, if it so desires, by direction, specify the content and method of making such communication to the complainant; <b>Provided also that in case of complaint originating due to registration of content template in wrong category, the content template shall be blacklisted by the OAP; and if five content templates of such sender are blacklisted for registration under wrong category, the OAP shall suspend the services of the sender, for one month or till such time all the content templates of the sender are reverified for registration under proper category,</b></p>	<p>Provided also that in case of complaint originating due to registration of content template in wrong category, the content template shall be blacklisted by the OAP; and inform to the registrar TSP, <del>and if five content templates of such sender are blacklisted for registration under wrong category, the OAP Registrar TSP shall blacklist suspend the services of the sender on DLT, for one month or till such time all the content templates of the sender are reverified for registration under proper category, whichever is later;</del> Registrar TSP to</p>	<p>Keeping the count of the blacklisted content template is not possible in current DLT as the registration of template and PE is on one DLT and traffic may have been sent by other TSPs DLT. Moreover if the OAP suspends the services of the PE on its DLT, PE may send the traffic form other DLT. So this is not practical.</p>	

		whichever is later;	reverify all the content templates of the sender for registration under proper category,		
		e) in case of occurrence of complained communication related to Voice Call from the series assigned for promotional call under sub-regulation (4)(b), further examine, within <del>one</del> three business days from the date of receipt of complaint by the OAP, whether all regulatory pre-checks were carried out in the reported case before delivering Unsolicited Commercial Communications; a			
(36)		e(ii) in case of non-compliance with the regulations, within two three business days from the date of receipt of complaint by the OAP, take action against the defaulting entity and communicate to TAP to inform the complainant about the action taken against his complaint as provided for in the Regulations and Code(s) of Practice:			
(37)		f) in case of occurrence of complained communications under clause (4)(b) related to promotional Voice Calls made using the number			

		<p>resource(s) allotted from series assigned for transactional and service calls, further examine within a maximum time of <del>two business hours</del> one business day, whether there are similar complaints or reports against the same Sender;</p>			
(38)		<p>i) <del>if it is found that the number of complaints against the Sender are from five or more than five unique Recipients during the last ten days,</del> if it is found that there are five or more complaints against the sender from unique recipients during the last ten days, immediately suspend the outgoing services of all the telecom resources of the sender which were utilized for sending UCC and simultaneously initiate investigation by issuing a notice to the sender, under <del>sub-regulation (5)(d)(i)</del> to give opportunity to the sender to represent the its case within five business days; thereafter investigate within five business days from the date of receipt of representation from the sender or expiry of the five business days period given to sender for</p>			

		<p>representing the case, whichever is earlier, and record the reasons of its findings. and if the conclusion of the OAP is that the sender was engaged in sending the Unsolicited Commercial Communications, it shall act against such sender as under</p>			
(39)		<p><del>Provided further that the Authority may specify different criteria for initiating action under sub-clauses (i) and (ii) above from time to time;</del> Provided further that the Authority may, from time to time, classify senders into different categories based on the parameters including, but not limited to,— (a) the importance of the entity to the economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/ disconnection of telecom resources on consumers; and may, accordingly, specify differentiated</p>			

		criteria for initiation of action and differentiated sets of enforcement measures applicable to such categories of Senders for violations of these regulations.			
(40)		5 b) OAP shall examine communication detail records (CDRs), within <del>one</del> two business days from the date of receipt of compliant <del>complaint</del> by OAP, to check the occurrence of complained communication between the complainant and the reported telephone number from which Unsolicited Commercial Communication was received;			
(41)		5 d) in case of occurrence of complained communications under <del>sub-regulation clause</del> (5)(b), OAP shall further examine within a maximum time of <del>two business hours</del> further one business day, <del>whether there are similar complaints or reports against the same Sender; and (i) if it is found that number of complaints against the Sender are from five or more than five unique Recipients during last ten days, OAP shall suspend the outgoing services of all the</del>			

		<p><del>telecom resources of the Sender irrespective of whether those telecom resources were actually used or not in making such communications and initiate an investigation as provided for in the sub-regulation (6);</del></p>			
(42)		<p>5di) if it is found that there are three or more complaints against the sender from unique recipients during the last ten days, and also any CLI allotted to the sender has been flagged or maintained as “Suspected UCC CLI” by the AI system of the access providers during these last ten days, OR, if there are five or more complaints against the sender from unique recipients during the last ten days, the OAP shall immediately suspend the outgoing services of the telecom resources of the Sender which were utilized for sending UCC and simultaneously initiate an investigation as provided for in the sub-regulation (6);</p>	<p>5di) if it is found that there are three or more complaints against the sender from unique recipients during the last ten days, and also any CLI allotted to the sender <b>by the OAP</b> has been flagged or maintained as “Suspected UCC CLI” by the AI system of the <b>OAP access providers</b> during these last ten days, OR, if there are five or more complaints against the sender from unique recipients during the last ten days, the OAP shall immediately suspend the outgoing services of the telecom resources of the Sender</p>		<p>The proposed process is creating two different actions on the senders of different TSPs. i.e. a TSP with AI Spam tagging system and a TSP without spam tagging system.</p> <p>A TSP with AI Spam tagging system is taking harsh action on its senders as compared to a TSP without AI spam tagging system.</p>

			<p>which were utilized for sending UCC and simultaneously initiate an investigation as provided for in the sub-regulation (6);</p>		
(43)		<p>5d(ii) in case, it is found that number of complaints against the sender are from less than five unique recipients during last ten days, <del>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:</del> and none of the CLIs of the sender has been flagged or maintained as “Suspected UCC CLI” by the AI system of the access providers during these last ten days, the OAP shall communicate to TAP to inform the complainant about the closure of complaint along with reasons in a manner specified in the Codes of Practice. Provided that the Authority may, if it so desires, by direction, specify the content and method of making such communication to the complainant: Provided further that the Authority may, from time to time, classify</p>			

		<p>senders into different categories and specify differentiated criteria for initiation of action against them under sub-clauses (i) and (ii) above, based on the parameters including, but not limited to (a) the importance of the entity to the economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/disconnection of telecom resources on consumers;</p>			
(44)		<p>in case of occurrence of complained communications under sub regulations (5)(d)(i) above, OAP shall, <b>immediately</b> issue a notice to the sender to give opportunity to represent <del>the case</del> its case within five business days; thereafter, shall <b>investigate within</b> five business days from the date of receipt of representation from the sender or expiry of the five business days period given to sender for representing the case, whichever is</p>			

		<p>earlier, and record the reasons of its findings and. If the conclusion of OAP is that the sender or its TM was engaged in sending the Unsolicited Commercial Communications, OAP shall take action against such sender as under-</p>			
(45)		<p>for the first instance of violation, outgoing services of all telecom resources allotted to the Sender including PRI/SIP trunks, SIMs etc. allotted to the sender shall be barred by all the Access Providers for a period of fifteen days, irrespective of whether those telecom resources were actually used or not in making such communications; (b) for the second and subsequent instances of violations, - (i) all telecom resources of the Sender including PRI/SIP trunks, SIMs etc. of the sender shall be disconnected by all the Access Providers for one year, irrespective of whether those telecom resources were actually used or not in making such communications; (ii) OAP shall put the Sender under the blacklist category during the period of one year as above and no new telecom</p>			

		resources shall be provided by any Access Provider to such Sender during this period;			
(46)		b iii) Provided further that the Authority may, from time to time, classify senders into different categories based on the parameters including, but not limited to,— (a) the importance of the entity to the economy or to a critical sector; (b) the criticality of services being delivered to consumers; (c) the nature and regulatory status of the entity; (d) the scale and volume of operations; (e) the extent and manner of usage of telecom resources; and (f) the potential impact of suspension/ disconnection of telecom resources on consumers; and may, accordingly, specify differentiated criteria for initiation of action and differentiated sets of enforcement measures applicable to such categories of senders for violations of these regulations.			
(47)	26	2A Every access provider shall maintain, record of every alleged violation of the regulations, reported by its customers within fifteen days			

		of the receipt of the unsolicited commercial communication by the customers, and shall also record reports of such alleged violations of the regulations received from the other terminating access providers.			
(48)		4A) For the purpose of audit of complaint handling process, the terminating and originating access providers shall provide the requested CDRs of the relevant period to the Authority.			
(48)	27 Consequences for failure to take action against curb the Unsolicited Commercial Communications from registered Senders or RTMs – (1) If an Access Provider fails to curb <del>Unsolicited Commercial Communications</del> to take action in accordance with the provisions of the 'Regulations' against Unsolicited Commercial Communications from registered Senders or RTMs, the Authority may impose financial disincentives on such Access Providers in each Licensed Service Area for each calendar month as under:				
(49)		27 a) without prejudice to any penalty which may be imposed under its licence or under any Act for the time being in force, OAP shall be liable to pay, by way of financial disincentive, an amount of one thousand rupees per count of valid complaint that is declared invalid: Provided that where UCC has originated due to Headers <del>and Content Templates</del> registered by another Access Provider in violation of the regulation thereon and OAP has taken action against such UCC as per regulation of these regulations, the financial	27 a) without prejudice to any penalty which may be imposed under its licence or under any Act for the time being in force, OAP shall be liable to pay, by way of financial disincentive, an amount of one thousand rupees per count of valid complaint that is declared invalid: Provided that where UCC has originated due to Headers and Content Templates registered by	OAP does not have the visibility on the content, so no FD should be imposed on OAP.	

		<p>disincentive at the rate of one thousand rupees per count of valid complaint <del>as above</del> shall be imposed on the Access Provider that has registered such Headers. <del>and Content Templates, instead of OAP</del> Provided further that where UCC has originated due to (i) wrong categorisation of Content Templates registered by the OAP, or, (ii) Content Templates registered under wrong category by another access provider and the traffic has been sent by the OAP under the wrong category, the financial disincentive shall be imposed at the rate of one thousand rupees per count of valid complaint on the OAP as well as the access provider that has registered such Content Templates under wrong category.</p>	<p>another Access Provider <b>or OAP</b> in violation of the regulation thereon and OAP has taken action against such UCC as per regulation of these regulations, the financial disincentive at the rate of one thousand rupees per count of valid complaint <del>as above</del> shall be imposed on the Access Provider that has registered such Headers. <del>and Content Templates, instead of OAP.</del></p>		
(50)	29) Representation by Senders or Telemarketers against the action taken by Access Providers.— (1)				
(51)	The Authority may on receipt of a complaint from the sender or telemarketer, within sixty days of action taken against it by the Access Provider under the regulations 25, if it considers	<p>if the Authority finds that conclusion of investigation by the Access Provider lacks adequate evidence against the sender or telemarketer,</p> <ul style="list-style-type: none"> <li>- (i) it may direct the Access Providers to restore all telecom resources of the sender or</li> </ul>			

	<p>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,</p>	<p>telemarketer and delete the name and address of such sender or telemarketer from the blacklist; (ii) may issue warning to the Access Provider for not exercising due diligence in deciding such cases</p> <p>Provided that while the sender or telemarketer may apply to the Authority for partial restoration of the telecom resources and removing the sender or telemarketer from the blacklist, the restoration charges payable by the sender or telemarketer shall not be less than half of the restoration charges calculated to restore all the telecom resources of the sender or telemarketer.</p>			
(52)	<p>34 A) Prohibition on blocking designated number series by Call Management Applications.— (1)</p>				
(53)	<p>No call management application or similar services for identification of UCC shall tag, block, filter, give any treatment to such calls different from those applicable for genuine communication or restrict</p>	<p>(2) Any call management app including phone dialers and third party apps, that offers the user of the app to report any Unsolicited Commercial Communication under any name such as spam, junk, etc., which implies UCC, shall send such report, in the manner and format as</p>			

	incoming calls <del>or messages</del> originating from any the designated number <del>series designated</del> for commercial communications, <del>as well as communication sent by the Government</del> , or facilitate blanket blocking of such communications as spam; (2) <del>Any Call Management Application that facilitates blanket blocking of such designated number series or tag it as spam shall be deemed non-compliant with these regulations: Provided that the consumers shall have the right to individually manage their own call through such Call Management Applications: Provided further that Authority may take appropriate enforcement measures, against non-compliant Call Management Applications in coordination with relevant authorities, if required.</del>	specified by the Authority from time to time to the DND registry maintained by the access providers. Provided that the Authority may prescribe the manner of sending such complaints by the call management apps to the DND registry maintained by the access providers.			
(54)	<del>Any Call Management Application that facilitates blanket blocking of such designated number series or tag it as spam shall be deemed non-compliant with these regulations: Provided that the consumers shall have the right to individually manage their own call through such Call Management Applications: Provided further that Authority may take appropriate enforcement measures, against non-compliant Call Management Applications in coordination with relevant authorities, if required.</del>	3) Any call management application or similar services that act in contravention of sub-regulation (1) and (2) shall be deemed to be non-compliant and in violation of these regulations;			
(55)	<del>Any Call Management Application that facilitates blanket blocking of such designated number series or tag it as spam shall be deemed non-compliant with these regulations: Provided that the consumers shall have the right to individually manage their own call through such Call Management Applications: Provided further that Authority may take appropriate enforcement measures, against non-compliant Call Management Applications in coordination with relevant authorities, if required.</del>	(4) The Authority may order/initiate action against any non-compliant call management application or similar service as follows: (i) The Authority may issue warning for the violations, and declare call management application or the service as non-compliant and violator; (ii) The Authority may initiate action under the relevant provisions of the IT Act, 2000, and the IT Rules, 2021, for the violation of the regulations. If the authority concludes that the call management application or similar service is non-			

		compliant, the IT intermediary shall be liable for losing exemption from liability of intermediary under IT Act 2000, and any other action as per the provisions of the IT Act, 2000. Provided that no order for action/ initiating action shall be made by the Authority, unless the concerned entity has been given a reasonable opportunity to represent			
(56)		35 i) any message transmitted by or on behalf <del>the directions</del> of the Central Government or State			
(57)		35 ii) any message transmitted by or on behalf <del>the directions</del> of bodies established under the Constitution;			
(58)	35A. The Terminating Access Provider (TAP) may charge the Originating Access Provider (OAP) upto Rs. 0.05 (five paisa only) per minute for A2P calls; Provided that there shall be no termination charge on: - (i) any A2P calls made by or on behalf of the Central Government or State Government; (ii) any A2P calls made by or on behalf of bodies established under the Constitution; (iii) any A2P calls made by or on the directions of		To be removed	This approach is not recommended because of the following reasons:  <b>1. Lack of Technical Mechanism for Traffic Segregation</b> The proposed approach is currently technically unfeasible. Telecom	

	<p>the Authority; (iv) any A2P calls made by any agency authorized by the Authority from time to time; (v) any A2P calls made by using number resources assigned from 140xx, 1600xx or any other series designated by the Authority for commercial communications from time to time.</p>			<p>Service Providers (TSPs) do not possess a standardized technical mechanism to distinguish A2P calls from P2P (Person-to-Person) calls at the point of origin. TSPs cannot identify at the outset whether a customer intends to use a service (be it LL, SIP/PRI, FTTH, Mobile, or VoIP) for manual dialling or automated dialling.</p> <p>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),</p>	
--	--	--	--	--	--

				<p>as each may classify the same traffic differently.</p> <p>It is requested that TRAI should include in the amendment a clear, standardized technical mechanism to segregate A2P and P2P traffic to prevent future inter-operator disputes.</p> <p><b>2. Economic Disincentives and Transparency Risks</b></p> <p>Imposing a mandatory termination charge of ₹0.05 per call for A2P traffic creates a significant price disparity between A2P and standard SIP/PRI connections.</p> <p>OAPs will be forced to raise tariffs for A2P calls</p>	
--	--	--	--	--	--

				<p>to cover these costs. This creates a "perverse incentive" for enterprise customers to misrepresent their usage as standard P2P to secure lower rates.</p> <p>This financial burden acts as a direct deterrent to the accurate registration of SIP/PRI connections, undermining the transparency and security goals of the Regulator.</p> <p>Therefore, It is requested to remove this clause to ensure that the registration process remains transparent and the financial burden does not drive traffic toward</p>	
--	--	--	--	--	--

				<p>"grey" or unverified routes.</p> <p><b>3. Necessity of Fixed Pricing for a Level Playing Field</b></p> <p>The proposal to set charges "up to ₹0.05" creates an uneven competitive landscape that favours dominant market players.</p> <p>A price range (₹0 to ₹0.05) allows TSPs with large customer bases to negotiate lower reciprocal rates amongst themselves, while smaller TSPs will be forced to pay the ceiling rate.</p> <p>This flexibility grants an unfair advantage to major TSPs, leading to</p>	
--	--	--	--	---	--

				<p>market consolidation and reduced competition.</p> <p>Therefore it is requested that the rate be fixed at exactly ₹0.05 or any other rate as decided by authority (not "up to") for A2P SMS also. A fixed, non-discriminatory rate ensures equal opportunity for all TSPs regardless of their subscriber base size.</p>	
	Schedule 1				
		<p><i>"35A. The Terminating Access Provider (TAP) may charge the Originating Access Provider (OAP) upto Rs.</i></p>		Same as above	

		<p><i>0.05 (five paisa only) per minute for A2P calls;</i></p> <p><i>Provided that there shall be no termination charge on: -</i></p> <p><i>(i) any A2P calls made by or on behalf of the Central Government or State Government;</i></p> <p><i>(ii) any A2P calls made by or on behalf of bodies established under the Constitution;</i></p> <p><i>(iii) any A2P calls made by or on the directions of the Authority;</i></p> <p><i>(iv) any A2P calls made by any agency authorized by the Authority from time to time;</i></p> <p><i>(v) any A2P calls made by using number resources assigned from 140xx, 1600xx or any other series designated by the Authority for commercial communications from time to time</i></p>			
(59)	4	c) linking of the entity with a unique mobile number: <i>Provided that the authority may, from time to time,</i>			

		prescribe any other manner of verification and authentication of the entities for the registration of senders and telemarketers by the access providers.			
(60)	2 h)	ensure that short code 127xxx, or any other code as prescribed by the Authority, shall be used by all Access Providers for sending consent seeking message related messages;			
(61)		(m) Primary Registration and Secondary validation of Content Templates for Service and Transactional Messages: (i) At the time of registration of SMS Content Templates, primary registration shall be undertaken by any one Access Provider, in accordance with the provisions of these regulations and the Directions issued by the Authority from time to time. The Sender shall clearly indicate, at the stage of primary registration, the intended category of commercial communication, namely Promotional, Service, Transactional or Government, and shall complete all applicable formalities at that stage; (ii) Upon	(m) Primary Registration and Secondary validation of Content Templates for Service and Transactional Messages: (i) At the time of registration of SMS Content Templates, primary registration shall be undertaken by any one Access Provider, in accordance with the provisions of these regulations and the Directions issued by the Authority from time to time. The Sender shall	Such Validation Is not possible on DLT, as the traffic may be sent to any of the TSP by a TM without prior intimation and as per the requirement of PE/TM.	

		<p>approval of a Content Template by the Access Provider undertaking primary registration, every other Access Provider shall, prior to acceptance of traffic, carry out secondary validation of the Content Template registered under Service and Transactional Message categories, by using the information available on DLT platform about such content template, for the limited purpose of verifying the correctness of its categorisation under these regulations. No additional documentation or procedural formality shall be required to be completed by the Sender for the purpose of secondary validation undertaken by other Access Providers: Provided that the Authority may, from time to time, prescribe the scope, manner and additional checks, if any, to be undertaken during such secondary validation, as well as the timelines for completion of secondary validation; (iii) Each Access Provider shall be independently responsible for ensuring compliance with these regulations</p>	<p>clearly indicate, at the stage of primary registration, the intended category of commercial communication, namely Promotional, Service, Transactional or Government, and shall complete all applicable formalities at that stage;.</p>		
--	--	---	---	--	--

		<p>and the directions of the Authority in respect of the categorisation of Content Templates accepted on its network, and also be liable for any breach thereof, irrespective of the categorisation approved by the Access Provider that has carried out the primary registration of such Content Template.</p>			
		<p>“(bh) “Service Message or Service Voice Call” means a message sent or voice call made by a Sender to –</p> <p>(i) its Customer or Subscriber to provide information pertaining to any product or service, its warranty, product recall, software upgrade alerts, safety or security of the product used or purchased by the Customer, periodic balance alerts, information regarding delivery of goods or services, and such Messages are not promotional in nature and do not require Explicit Consent; or</p>			<p>Regarding the scenario of <b>explicit consent</b>, we propose that such consent should not be integrated into the <b>Customer Relationship Form (CRF)</b>. Implementing this at the TSP level is technically unfeasible as TSPs lack the visibility to identify exactly when a specific transaction is initiated. We require further clarity on the</p>

		<p>(ii) a Recipient to facilitate or complete a commercial transaction involving the ongoing purchase or the use by the Recipient of the product or services offered by the Sender after obtaining Explicit Consent from the Recipient and such Messages are not promotional in nature:</p> <p>Provided that such Explicit Consent shall be for seven days or as directed by the Authority from time to time</p> <p>Provided further that a transactional Message or transactional Voice Call containing information pertaining to service shall be treated as a Service Message or Service Voice Call;”; amended dated 12.05.25</p>			<p>operational workflow. However, it is our position that the <b>Principal Entity (PE)</b> must bear the responsibility for compliance, ensuring that any communication based on explicit consent is transmitted within a <b>7-day window</b> of the initial transaction or consent acquisition</p>
--	--	--	--	--	---